Department of Health and Human Services

PRIVACY MANUAL

Prepared by the Privacy and Security Office

Rev 6/2020

Table of Contents

Chapter 1: Introduction to the Privacy Program *6*

1.1 Purpose **6**
Format 6

1.2 Approach **6**
1.2.1 Alignment with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) 6
1.2.2 Alignment with the statutory authority for confidentiality of substance use disorder patient records; Title 42, Part 2 Confidentiality of Substance Use Disorder Patient Records 6
1.2.3 Alignment with Information Payment Card Industry Data Security Standard (PCI DSS) 6
1.2.4 Alignment with Criminal Justice Information (CJI) 7
1.2.5 Alignment with Federal Tax Information (FTI) 7
1.2.6 Alignment with Family Educational Rights and Privacy Act (FERPA) 7

1.3 Applicability **7**

1.4 Enforcement **7**

Chapter 2: HIPAA Administrative Requirement Policies

..... *8*

2.1 Policy Management **8**
2.1.1 Department-wide Policies 8
2.1.2 DHHS Division/Office Responsibility (Procedures) 8
2.1.3 Retention and Disposition 8
2.1.4 Compliance 8
2.1.5 Implementation 8
2.1.6. Maintenance 9

2.2 Privacy Official **9**

2.3 Workforce **10**
2.3.1 Training 10
2.3.2 Confidentiality Agreement 11
2.3.3 Identification 11
2.3.4 Sanctions 11

2.4 HIPAA Safeguards **12**
2.4.1 Safeguards 12
2.4.2 Administrative Safeguards 13
2.4.3 Physical Safeguards 16
2.4.4 Technical Safeguards 18

2.5 HIPAA Hybrid Entity Designation **19**
2.5.1 Initial Coverage Determination 20
2.5.2 Subsequent Coverage Determination Notification 20
2.5.3 Segregation of Functions 20

Chapter 3: HIPAA Use and Disclosure Policies

..... *20*

3.1 HIPAA Use and Disclosures **20**
3.1.1 Permitted Uses and Disclosures 21
3.1.2 Permitted Uses and Disclosures with Client Authorization 21

3.1.3 Business Associate Disclosures 22
3.1.4 Deceased Client 22
3.1.5 Personal Representative Disclosures 22
3.1.6 Confidential Communications 22
3.1.7 Disclosures by Whistleblowers and Workforce Member Crime Victims 22
3.1.8 HIPAA Use and Disclosures Treatment, Payment, and Health Care Operations 22
3.1.9 Use and Disclosures Requiring An Individual Opportunity to Agree or Object 24
3.1.10 Disaster Relief 25
3.1.11 Required by Law 25
3.1.12 Public Health Activities 26
3.1.13 Communicable Disease Notification 27
3.1.14 Child Abuse and Neglect Reporting 27
3.1.15 FDA-Regulated Product or Activity Monitoring 27
3.1.16 Work-related Illness or Injury Monitoring and Workplace Medical Surveillance 27
3.1.17 Adult Abuse and/or Neglect Reporting 27
3.1.18 Health Oversight Activities 28
3.1.19 Judicial and Administrative Proceedings 29
3.1.20 Law Enforcement Purposes 29
3.1.21 Specialized Government Functions 31
3.1.22 Personal Representative 32
3.1.23 Client Photographs 32
3.1.24 Psychotherapy Notes 32
3.1.25 Verification 33
3.1.26 Incidental to an Otherwise Permitted Use and Disclosure 33

3.2 Authorizations 33
3.2.1 Standard Authorization Format 34
3.2.2 Signatures 36
3.3.3 Dates 36
3.3.4 Revocation of Authorization 36
3.3.5 Retention Period 37
3.3.6 Photocopy/Facsimile Authorization 37
3.3.7 Contractor Authorizations 37

3.3 Consent for Treatment, Payment, and Health Care Operations 37
3.3.1 Consent 37
3.3.2 DMH/DD/SAS 38
3.3.3 Consent Form 38
3.3.4 Exceptions 38

3.4 Minimum Necessary 39
3.4.1 Minimum Necessary within NC DHHS 39
3.4.2 Minimum Necessary Outside NC DHHS 39
3.4.3 Minimum Necessary for Routine Use or Disclosure 40
3.4.4 Minimum Necessary for Non-Routine and Other disclosures 40

3.5 De-Identification of Health Information and Limited Data Sets 41
3.5.1 Protected Health Information Individual Identifiers 41
3.5.2 De-Identification 42
3.5.3 Limited Dataset 42
3.5.4 Exclusion of Data Elements Considered to be Identifying Elements 43
3.5.5 Reidentification 45
3.5.6 Data Use Agreement 45
3.5.7 Elements Permitted in De-Identified Health Information and Limited Data Sets 46

3.6 Research 48
3.6.1 Researchers External to DHHS 48
3.6.2 Institutional Review Boards IRB 49

3.6.3 Research Conducted with Client Authorization 49
3.6.4 Alteration or Waiver of Client Authorization to Use or Disclose Individually Identifying Health Information for Research 50
3.6.5 De-Identified Health Information 51
3.6.6 Use of Limited Data Sets in Research 51
3.6.7 Research Requests Received from Organizations External to DHHS 52
3.6.8 Retention of Research Documentation 53

3.7 Marketing and Fundraising 53
3.7.1 Permitted Communications Not Considered Marketing 53
3.7.2 Fundraising Activities 54
3.7.3 Authorizations 54

3.8 Alternative Confidential Communications 54
3.8.1 Denial Requests and Exceptions 55

3.9 Verification of External Requestors 56
3.9.1 Patient or Patient Representative Requestors 56
3.9.2 Third-Party Requestors 56
3.9.3 Third-Party Requestors 56
3.9.4 Third-Party Requestors 56

3.10 Legal Occurrences 56
3.10.1 Use and Disclosure Enforceable by Court of Law 57
3.10.2 Preemption 57
3.10.3 Authorization 58
3.10.4 Authorization Not Required 58
3.10.5 Accounting of Disclosures 60

Ch. 4 Client Rights Policies

..... 60

4.1 Notice of Privacy Practices 60
4.1.1 General Notice Requirements 61
4.1.2 Notice of Privacy Practices Required Elements 62
4.1.3 Additional Privacy Notice Requirements (Health Care Plan) 63
4.1.4 Additional Privacy Notice Requirements (Health Care Providers That Have Direct Treatment Relationship with Clients) .. 64

4.2 Rights of Clients 65
4.2.1 Right to Confidential Communications 66
4.2.2 Right to Adequate Notice of Use and Disclosure of Individually Identifiable Health Information 66
4.2.3 Right to Obtain Paper Copy after Electronic Notice 67
4.2.4 Right to Request Access to Individually Identifiable Health Information 67
4.2.5 Right to Request Amendment to Individually Identifiable Health Information 69
4.2.6 Right to Accounting of Disclosures of Individually Identifiable Health Information 71
4.2.7 Right to Request Privacy Restrictions for Individually Identifiable Health Information 72
4.2.8 Client Requests 73
4.2.9 Department Assurance and Procedures 73
4.2.10 Agreement or Denial of a Request for Restriction 73
4.2.11 Client Right to File a Complaint 75

4.3 Personal Representatives 75
4.3.1 Unemancipated Minors 76
4.3.2 Deceased Client 77
4.3.3 Exceptions 78

4.4 Designated Record Sets 78

4.5 Accounting of Disclosures 81
4.5.1 Disclosure Exclusions/Inclusions 81

4.5.2 Tracking Disclosures 82
4.5.3 Request for Accounting of Disclosures 83
4.5.4 Providing Accounting of Disclosures to Client or Personal Representative 83
4.5.5 Providing Accounting of Disclosures to health oversight agencies or law enforcement 84
4.5.6 Request of Accounting for DMH/DD/SAS facilities. 84
4.5.7 Contents of the Accounting of Disclosures to Clients or Their Personal Representatives 85
4.5.8 Multiple Disclosures 85
4.5.9 Research Disclosures 85
4.5.10 Business Associates Disclosures 86
4.5.11 Retention 86

Ch. 5 Security Rule Policies

..... 87

5.1 Business Associates (Internal/External) 87
5.1.1 Business Associate Agreements 88
5.1.2 Identifying Internal and External Business Associates 89
5.1.3 Contractual Documentation Requirements 91
5.1.4 Termination of Business Associate Relationship 91
5.1.5 Tracking of Business Associates 91
5.1.6 Training 92

5.2 Acceptable Use of DHHS Information Systems 92
5.2.1 Roles and Responsibilities 92
5.2.2 Rights of Information Ownership 92
5.2.3 Rules of Acceptable Use 93
5.2.4 Prohibited Uses 93
5.2.5 Requirements 94
5.2.6 User Privacy 94
5.2.7 Software License Agreements 94

5.3 ZixMail Usage Policy 96

Ch. 6. Breach and Complaints 96

6.1 HIPAA Breach Notification of Unsecured PHI 96
6.1.1 Administrative Requirements 97
6.1.2 Reporting HIPAA Incidents and Complaints 97
6.1.3 Review by DHHS PSO and DHHS Office of General Counsel 98
6.1.4 Evaluating a HIPAA Incident or Complaint 98
6.1.5 Notification 100
6.1.6 Retention of Breach Notice Documentation 102
6.1.7 Reporting of Incident to DHHS by Business Associate 102
6.1.8 Overlapping Incidents and Complaints 103

6.2 Privacy Incident and Complaint Reporting 103
6.2.1 Reporting Incidents and Complaints 103
6.2.2 Documenting, Investigating, and Resolving Incidents and Complaints: 104
6.2.3 Types of Incidents and Complaints 105

Ch. 7 Identity Theft Policies

..... 106

7.1 Identity Theft Red Flags and Address Discrepancy Policy 106
7.1.1 Red Flag and Address Discrepancy Policy 106
7.1.2 Financial Institution or a Creditor That Owns or Maintains Covered Accounts 106
7.1.3 Debit/Credit Card Issuer 106

7.1.4 User of a Consumer Report 106
7.1.5 Identity Theft Prevention Program 107

7.2 Identity Theft and Security Breach Notification 108
7.2.1 Collection, Usage, Storage, Transmission, Mailing, Disclosure and Destruction 109
7.2.2 Security Breach 110
7.2.3 Reporting of Incident by a Non-DHHS Organization 112
7.2.4 Complete Risk Assessment 112
7.2.5 Duty to Notify the Attorney General's Office 113
7.2.6 Duty to Report to both the Attorney General's Office and Consumer Reporting Agencies. 113
7.2.7 Duty to Report to the General Assembly 114
7.2.8 Communications with the Media or Outside Agencies 114

CHAPTER: NC DHHS Privacy Manual Updates 116

Chapter 1: Introduction to the Privacy Program

1.1 Purpose

NC DHHS is entrusted with millions of documents containing confidential personal and health information of its program recipients, clients and workforce members. There are various regulations that require HIPAA-covered, non-covered, or hybrid DHHS Divisions and Offices to implement appropriate protections for handling confidential or sensitive data. To ensure compliance with HIPAA and other federal, department and state regulations and standards, any sensitive data, internal proprietary and confidential data, DHHS also requires its DHHS Divisions and Offices that use, collect, disclose, or store confidential information to implement applicable safeguards. The purpose of the privacy manual is to offer a guide for the North Carolina Department of Health and Human Services (NC DHHS) divisions, facilities and schools as they work towards protecting their clients. For purposes of this manual the term "Department" is used to describe NC DHHS.

Format

For purposes of this manual, the format includes Chapter (X), Section (X.X), Subsections (X.X.X), Guidelines, and Guidance.

- Chapters are groupings of related policies.
- Sections are related policies within the Chapter and include the purpose statement.
- Subsections are various subjects within the policy.
- Guidelines are the overall policy statements.
- Guidance are the procedural related statements.

1.2 Approach

The Department shall ensure compliance with privacy and confidentiality requirements through the development and implementation of privacy guidelines that specify the Department's methods for the protection of Protected Health Information (PHI), Personally Identifiable Information (PII) and any other confidential information. The requirements in these policies shall be based on many business practices already employed by NC DHHS divisions, facilities and schools. In addition, privacy policies shall include other federal and state law requirements that have an impact on the use and disclosure of health information. Most federal and state laws that are more stringent than the HIPAA requirements will generally remain in effect and will not be preempted by HIPAA. In addition, some state laws such as categories of laws that provide for reporting of disease or injury, child abuse, birth or death and other laws requiring disclosure of individually identifiable health information will remain in effect.

1.2.1 Alignment with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH)

The HIPAA Privacy Rule establishes a set of national standards for the protection of certain health information. It addresses the use and disclosure of Protected Health Information (PHI) by covered entities, standards for individual privacy rights. The Office of Civil Rights (OCR) is responsible for implementing and enforcing the Privacy Rule.

The HIPAA Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.

The NC Office of Attorney General has determined that NC DHHS meets the definition of a "hybrid entity" and has both covered health care components and non-covered health care components within its department. DHHS, as a hybrid entity, is responsible for designating which of its DHHS Divisions and offices are covered health care components and for ensuring that those components comply with HIPAA.

1.2.2 Alignment with the statutory authority for confidentiality of substance use disorder patient records; Title 42, Part 2 Confidentiality of Substance Use Disorder Patient Records

The regulation imposes restrictions upon the disclosure and use of substance use disorder patient records which are maintained in connection with the performance of any part 2 program.

1.2.3 Alignment with Information Payment Card Industry Data Security Standard (PCI DSS)

PCI Data Security Standard (PCI DSS) is a set of security controls that businesses are required to implement to protect credit card data.

1.2.4 Alignment with Criminal Justice Information (CJI)

Criminal Justice Information (CJI) includes biometric data, identity history data, biographic data specific to a unique case, property data, and incident history or criminal history data.

1.2.5 Alignment with Federal Tax Information (FTI)

Federal Tax Information (FTI) includes data that the IRS obtains from any source or developed through any means that relates to potential liability of any person under the IRC, information extracted from a return, including names of dependents or the location of a business, and the taxpayer name, address, and identification number.

1.2.6 Alignment with Family Educational Rights and Privacy Act (FERPA)

Federal Educational Rights and Privacy Act information includes directory data of the student's name, address, phone number, date and place of birth, honors and awards, dates of attendance.

1.3 Applicability

Unless denoted by applicability, all sections and subsections of this manual are required by all DHHS Divisions and Offices.

1.4 Enforcement

For questions or clarification on any of the information contained in this policy, for general questions about department-wide policies and procedures, contact the **DHHS PSO Policy Writer.**

-- Remainder of Page Intentionally Left Blank --

2.1 Policy Management

DHHS shall develop policies that are appropriate for its DHHS Divisions and Offices to implement in order to protect the privacy of individually identifiable health information that is created, received, and maintained during its regular course of business. Policies will be reasonably designed to comply with state and federal laws, considering the scope of the requirement and the nature of activities undertaken that relates to individually identifiable health information. The HIPAA Privacy Rule will be the primary resource for DHHS privacy policies.

2.1.1 Department-wide Policies

DHHS shall evaluate each privacy policy based primarily on the HIPAA Privacy Rule to determine if the policy should be applied to all DHHS Divisions and Offices within the department regardless of the HIPAA impact. Determination, by the DHHS Office of the Secretary, for a department-wide approach to policy requirements will take into account the most efficient and effective methods for ensuring the protection of individually identifiable health information and equitable client rights, while promoting consistency in the management of health information throughout the department.

2.1.2 DHHS Division/Office Responsibility (Procedures)

It is the responsibility of DHHS Divisions and Offices to develop procedures for implementing policies for which they must comply. Because DHHS Divisions and Offices conduct their business operations somewhat differently, specific procedures for implementing department privacy policies must be developed at the DHHS Division and Office level. Required procedural elements to be addressed by DHHS Divisions and Offices will be identified by the Department under the "Guidance" section of the policy or available on the internal share drive supported by the Privacy and Security Office.

2.1.3 Retention and Disposition

Policies, procedures, and privacy documentation required by the HIPAA Privacy Rule must be maintained in writing in accordance with the General Schedule for State Agency Records issued by the North Carolina Department of Cultural Resources, Division of Archives and History, Archives and Records Section, Government Records Branch. Additionally, 45 CFR 164.316(b)(2)(i) requires DHHS Divisions and Offices to "retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later."

2.1.4 Compliance

DHHS Divisions and Offices must comply with the privacy policies developed and implemented according to this process by April 14, 2003. This date represents the compliance date specified in the HIPAA Privacy Rule. Divisions and Offices must follow NC DHHS PSO policies and procedures in accordance with the 45 CFR § 164.530 - Administrative requirements under HIPAA.

2.1.5 Implementation

The Department shall develop policies that address essential administrative privacy requirements so DHHS Divisions and Offices will use and/or disclose individually identifiable health information in a confidential and secure manner. All policies shall be located in the DHHS Policy and Procedure Manual that is maintained by the Office of the DHHS Secretary. The policies to be developed will address the following privacy requirements:

- Policy and Procedure Changes
- Privacy Officer
- Workforce
- Safeguards
- Business Associates
- Minimum Necessary
- Use and Disclosure
- Client Rights
- Sanctions
- Privacy Incident and Complaint Reporting
- Consent and Authorizations
- Use and Disclosures
- Personal Representatives

- Notice of Privacy Practices
- De-Identification and Limited Data Sets

2.1.6. Maintenance

The Department shall review policies annually for updates as needed. New policies shall be published after approvals have been obtained from leadership. New, revised, and removed policies shall be documented in the Privacy Manual Update log located in the final chapter of this manual.

2.2 Privacy Official

The HIPAA Privacy Rule requires the designation of personnel who are responsible for the implementation of privacy policies and procedures, as well as personnel who are responsible for receiving complaints and answering questions concerning privacy. DHHS, as a hybrid entity, must designate a privacy officer who is responsible for the coordination and implementation of all privacy and confidentiality efforts within the department. In addition, DHHS has determined that the department DHHS Divisions and Offices that are defined in the purpose section of this policy must each designate a privacy official to act as the primary point of contact for the privacy of health information that is used within or disclosed outside of that DHHS Division and Office. The DHHS Privacy Officer and DHHS Division and Office Privacy Officials are responsible for the coordination and facilitation of compliance activities associated with departmental privacy policies.

Guidelines

The DHHS Privacy Officer is designated by the Secretary of the DHHS. The DHHS Privacy Officer shall maintain the list of all DHHS Division and Office privacy officials within the department. The DHHS Privacy Officer shall oversee all activities related to the development, maintenance and adherence to department policies regarding the use and disclosure of individually identifiable health information, in accordance with state and federal laws as well as best business practices. The responsibilities of the DHHS Privacy Officer shall also include, but are not limited to, the following:

- Act as the Department expert for issues related to privacy in the use and disclosure of health information.
- Serve as liaison with the North Carolina Office of the Attorney General in the analysis and application of state and federal privacy laws.
- Develop and maintain Department privacy policies related to the use and disclosure of health information.
- Provide guidance in the implementation of health information privacy policies and procedures.
- Provide consultation and direction regarding privacy and confidentiality of health information to DHHS Divisions and Offices within the Department.
- Coordinate privacy activities within the department.
- Create educational awareness programs and ensure staff and extended workforce training is conducted.
- Monitor state and federal privacy legislation.
- Monitor DHHS compliance with DHHS privacy policies and report compliance level to management.
- Escalate privacy issues to DHHS management as appropriate.
- Communicate all Department expectations for privacy to DHHS Division and Office Privacy Officials.

DHHS Division and Office Privacy Officials: Privacy Officials shall guide all activities related to adherence to DHHS privacy policies regarding the use and disclosure of individually identifiable health information, in accordance with state and federal laws, best business practices, and under the direction of the DHHS Privacy Officer.

DHHS Division and Office Privacy Official responsibilities shall also include, but are not limited to, the following:

- Serve as primary contact for privacy issues and concerns regarding the use and disclosure of health information and for client rights regarding health information.
- Serve as the liaison to the DHHS Privacy Officer for privacy-related activities.
- Coordinate and facilitate efforts to support the DHHS Division and Office in the accomplishment of their privacy compliance activities.
- If the DHHS Division and Office is also a covered health care component under the HIPAA Privacy Rule (i.e., not an internal business associate), the DHHS Division and Office Privacy Official shall be responsible for responding to client requests for further information concerning the Notices of Privacy Practices.

Each DHHS Division and Office defined in the purpose section of this policy shall designate a staff member to serve as its privacy official. These designees may have other primary job functions in addition to privacy responsibilities. The privacy officer will work closely with the HIPAA Coordinator when there is an incident investigation or breach involving HIPAA data. Organizationally, privacy

officials report to their supervisor within the DHHS Division and Office. DHHS Division and Office Privacy officials shall have an indirect reporting relationship to the DHHS Privacy Officer for privacy-related activities only. Upon request from the DHHS Division and Office supervisor, the DHHS Privacy Officer shall provide input into its privacy official's annual performance evaluation as applicable to privacy-related activities.

2.3 Workforce

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule addresses the protection of individually identifiable health information and mandates that covered entities provide appropriate privacy training to their workforce and extended workforce on the DHHS Division and Office's policies and procedures regarding protected health information.

The HIPAA Privacy Rule also requires that appropriate sanctions be established for the workforce and extended workforce for failure to comply with privacy requirements, including making reasonable efforts to lessen any resulting harmful effects of unauthorized use or disclosure of information.

DHHS has determined that every DHHS Division and Office in the department that maintains individually identifiable health information must comply with this workforce policy to ensure that members of the DHHS workforce and extended workforce understand the importance of privacy protections and the consequences of inappropriate uses or disclosures of individually identifiable health information.

Guidelines

DHHS Divisions and Offices shall ensure that members of their workforce and extended workforce make reasonable efforts to protect individually identifiable health information from intentional or unintentional use or disclosure that is in violation of the department's privacy policies and/or DHHS Divisions and Offices' procedures. In the event that an agency should become aware of a privacy policy violation, the agency must make reasonable efforts to lessen any resulting harmful effects. Each agency shall ensure the protection of individually identifiable health information in a manner consistent with all requirements specified within this policy.

This policy shall address the North Carolina Department of Health and Human Services (NC DHHS) privacy requirements regarding the use and disclosure of individually identifiable health information by full time and part time employees, hereinafter referred to as "workforce". Additionally, this policy covers students, volunteers, trainees, contractors, personnel working through a temporary agency, and other persons whose conduct in the performance of work for an agency is under the direct control of the agency, whether or not they are paid by the agency, who are hereinafter referred to as "extended workforce".

2.3.1 Training

Privacy and Security training is available to all employees on the LMS system and must be completed on an annual basis. DHHS Divisions and Offices shall ensure that its workforce and extended workforce are trained with respect to the protection of individually identifiable health information in accordance with DHHS Division and Office policy and procedures, as appropriate in the performance of their job responsibilities. Training shall be provided to workforce/extended workforce who have direct, inadvertent, or incidental access to such health information. Basic privacy training must include the following:

- Awareness of vulnerabilities of Protected Health Information (PHI) and Personally Identifiable Information (PII) in each DHHS Division and Office's possession
- Procedures that ensure the protection of PHI and PII as necessary for each individual to carry out his/her job function
- Consequences for violation of privacy policies or procedures
- Documentation and retention of training attendance shall be retained for no less than six (6) years from the last date of the individual's active participation as a member of the workforce or extended workforce. Contractor staff that are managed by the DHHS Division and Office and under a departmental contract, the department contract administrator shall retain the training documentation. The training documentation shall include;
    - Workforce member name, job title, date of training, and type of training (basic, comprehensive).

When a change is made to DHHS Privacy Policies, or and Office procedure, each workforce member whose function(s) are impacted by the change shall receive the instruction necessary to implement the change within a reasonable amount of time after the change becomes effective.

2.3.2 Confidentiality Agreement

All current DHHS Division and Office workforce/extended workforce members shall be required to sign a Confidentiality Agreement acknowledging their understanding of the and Office's privacy policies and procedures as well as the consequences of any violation. The agreement shall be signed within a reasonable amount of time after employment, but no later than upon completion of privacy training. Confidentiality Agreements shall be retained for at least as long as the individual remains a member of the workforce or extended workforce.

2.3.3 Identification

DHHS Divisions and Offices including HIPAA Covered, Hybrid, DHHS Internal HIPAA Business Associates, and any DHHS Division and Office that performs oversight or other services for a DHHS HIPAA covered entity shall require DHHS Division and Office workforce and extended workforce to wear some form of visible identification when performing job responsibilities for that DHHS Division and Office. An DHHS Division and Office that promotes a residential environment for their clients may be excluded from staff identification at the discretion of the appropriate DHHS Division and Office management.

Each DHHS Division and Office must determine a reasonable method of employee identification. The method need not be costly. When workforce or extended workforce members conduct business in person that is likely to include the sharing of an individual's health information, the workforce/extended workforce member shall prominently display official DHHS Division and Office identification that contains the member's name.

2.3.4 Sanctions

Sanctioning against employees who fail to comply with DHHS privacy policies and/or DHHS Division and Office procedures shall be in accordance with the State Human Resources Act and related personnel policies, except that the sanctions for educators subject to Chapter 11C of the North Carolina General Statutes (N.C.G.S.) shall be in accordance with N.C.G.S. § 115C-325. Appropriate sanctions for noncompliant contractors and other workforce members who are not state employees shall be imposed consistent with the terms of their contracts or operative working agreements.

DHHS Divisions and Offices must review each incident individually, taking into consideration the severity of the incident, circumstances surrounding the incident, the harm done to the client and to the DHHS Division and Office, and any possible repercussions as a result of the use or disclosure made by staff. All instances of sanctioning shall be documented through existing personnel processes. The DHHS Privacy Officer and DHHS Division and Office Privacy Official, if one is designated in the DHHS Division and Office, shall be notified of any privacy violations and, to the extent permitted by law, any sanctions applied.

DHHS Divisions and Offices shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the following reasons:

- exercising his/her privacy rights
- participating in any process relating to privacy compliance
- filing a complaint with the Secretary of the U.S. Department of Health and Human Services
- participating in a privacy related investigation, privacy compliance review, proceeding, or hearing; or
- engaging in reasonable opposition to any act or practice that the person believes to be unlawful as long as the action does not involve disclosure of individually identifiable health information

Retaliation shall not occur for individuals who make a disclosure to a health oversight DHHS Division and Office, public health authority, or an attorney retained by or on behalf of the individual to determine legal options, provided that the individual believes in good faith that an DHHS Division and Office has done any of the following:

- performed an unlawful act
- violated professional or clinical standards; or
- endangered a client or the public through the care, services, or conditions provided

An DHHS Division and Office is not considered to have violated HIPAA Privacy Rules if a member of its workforce or extended workforce who is the victim of a criminal act discloses individually identifiable health information to a law enforcement officer about the suspected perpetrator and the health information is the minimum needed to appropriately address the criminal act.
All business practices shall provide for preventing intentional unauthorized disclosure of individually identifiable information to unauthorized parties through written or oral interactions, as well as minimizing unintentional conveyance. Business practices shall also provide for reasonable efforts to lessen any resulting harmful effects in the event that an DHHS Division and Office should become aware of a HIPAA Privacy Rule violation by the DHHS Division and Office or its business associate.

2.4 HIPAA Safeguards

The HIPAA Privacy Rule requires covered health care components to implement appropriate administrative, physical, and technical safeguards to avoid unauthorized use or disclosure of individually identifiable health information. DHHS Divisions and Offices are not asked to "guarantee" the safety of individually identifying health information against all imaginable assaults; instead, DHHS Divisions and Offices are instructed to use protections that are flexible, scalable, and provide reasonable safeguards. The safeguards implemented in different DHHS Divisions and Offices will vary depending on factors such as DHHS Division and Office size and the nature of its business. To implement reasonable safeguards, each DHHS Division and Office should analyze its own needs and circumstances such as the nature of the information it holds and assess potential risks to a client's privacy. DHHS Divisions and Offices should also consider the potential impacts on client care and other issues such as the financial and administrative burdens of implementing various safeguards.

Safeguards addressed in DHHS Privacy Policies include the administrative, physical, and technical protections necessary for safeguarding individually identifying health information as it is found in the working environment (e.g., oral communications, paper records, medical supplies/equipment, computer screens, etc.).

Guidelines

The purpose of this policy is to establish privacy safeguards that protect individually identifiable health information from unauthorized use or disclosure and to further protect such information from tampering, loss, alteration, or damage. It is not the intent of this policy to address all the safeguards necessary to protect electronic data containing individually identifiable health information since those safeguards are included in the Department of Health and Human Services (DHHS) Security Policies. The policy is applicable to the following types of DHHS Divisions and Offices:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered health care components including Hybrid DHHS Divisions and Offices
- Internal business associates; and
- Non-covered health care components that maintain individually identifiable health information

2.4.1 Safeguards

DHHS has determined that the requirement to safeguard confidential health information should be extended to all DHHS Divisions and Offices within the department that maintain individually identifiable health information.

- **Administrative Safeguards**

DHHS Divisions and Offices shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each DHHS Division and Office. Confidential information that is transmitted by facsimile (fax) machines, e-mail, printers, copiers, and by telephone or other oral means of communication shall be protected from unauthorized use and disclosure. DHHS Divisions and Offices shall:

  - Address measures to direct the conduct of DHHS Division and Office staff in relation to the protection of individually identifiable health information; and
  - Develop and implement DHHS Division and Office safeguard procedures.

- **Physical Safeguards**

DHHS Divisions and Offices shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each DHHS Division and Office by establishing protections used for equipment/supplies/records/work areas to prevent unauthorized use or disclosure of individually identifiable health information maintained by the DHHS Division and Office.

- **Technical Safeguards**

DHHS Divisions and Offices shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each DHHS Division and Office by addressing technical safeguards used for accessing confidential information maintained in computer systems and other electronic media through identification of staff who need access to electronic data and control of access through the use of unique user identifiers and passwords.

Guidance:

- **Mail or hand delivery**
  Whenever feasible, documents containing individually identifiable health information should be hand delivered or mailed using the United States Postal Service (USPS), courier, or other delivery service. All documents containing individually identifiable health information shall be placed in a secure container (e.g., sealed envelope, lock box) that is labeled "Confidential", addressed to the recipient, and include a return name and address. When transmitting individually identifiable health information via interoffice mail, the information shall be placed in a sealed envelope and then placed in an interoffice envelope.

- **Facsimile**
  DHHS Divisions and Offices must designate specific fax machines that will be used to send and/or receive documents containing individually identifiable health information. Where possible, fax machines should be strategically located near the intended recipient(s) of the health information.

  Incoming fax transmissions of documents that contain individually identifiable health information must be protected from unauthorized disclosure to staff or others who are not authorized to access the information. Each DHHS Division and Office must determine the methods to be used in that DHHS Division and Office to ensure the protection of incoming individually identifying health information via fax transmission. Staff should request that those faxing confidential information to the DHHS Division and Office call in advance to schedule the transmission.

  Efforts to protect outgoing fax transmission of documents containing individually identifiable health information shall be initiated by DHHS Division and Office staff as listed below;
  - Prior to faxing such documents, DHHS Division and Office staff shall attempt to schedule the transmission with the recipient so that the faxed document can be promptly retrieved by the recipient.
  - Whenever feasible, routine destination fax numbers should be pre-programmed into fax machines. DHHS Divisions and Offices shall test pre-programmed numbers at regular intervals (e.g., monthly) to reduce transmission errors.
  - DHHS Divisions and Offices should request that routine recipients of faxed documents containing IIHI inform the DHHS Division and Office immediately if their fax number(s) change so that DHHS Division and Office records and pre-programmed numbers can be updated accordingly.
  - Staff authorized to send faxes with individually identifiable health information shall check the recipient's fax number before transmittal and shall confirm delivery via telephone or review of the confirmation sheet of fax transmittal.
  - DHHS Divisions and Offices shall implement procedures for maintaining and reviewing fax transmittal summaries and confirmation sheets.
  - In the event of a misdirected fax, the recipient must be contacted immediately and shall be asked to destroy the information by burning or shredding the document. Misdirected faxes are considered accidental disclosures and must be accounted for in accordance with DHHS Privacy Policy, Use and Disclosure Policies, Accounting of Disclosures. In addition, the DHHS Division and Office shall use the approved electronic reporting process referenced in the Privacy Incident and Complaint Reporting policy.
  - DHHS Divisions and Offices shall include a confidentiality statement on all fax cover sheets.

  In addition to the required confidentiality statement, the fax cover sheet should contain:
  - Sender's name, mailing address, e-mail address, telephone number, and fax number;

- Recipient's name, telephone number, and fax number;
- Number of pages transmitted, including coversheet; and
- Instructions for verification of fax receipt (e.g., phone call to sender to confirm receipt of the document).

- **Email**

  Emails containing individually identifiable health information should be both encrypted and password protected. An automatic delay should be placed on all employee and staff email systems forcing the emails to wait in queue prior to being sent. DHHS Divisions and Offices need to be aware that:

  - Email is considered public record, but confidential information contained in or attached to an e-mail can be protected from public disclosure in accordance with NCGS 132-6(c).
  - E-mails containing individually identifying health information can be forwarded by the recipient to someone not authorized to have access to the information; therefore, DHHS Divisions and Offices shall only transmit e-mails containing individually identifiable health information to persons within DHHS who are knowledgeable about DHHS Privacy Policies, to business associates, or to other covered entities (e.g., health plans, health care providers).
  - All efforts should be made to avoid using e-mail for particularly sensitive matters (e.g., HIV status, psychiatric disorders) and time-sensitive messages (e.g., appointment scheduled for next day).
  - Avoid including individually identifiable health information in the subject line or body of an e-mail. If it is essential for the efficiency of business operations to send individually identifiable health information via e-mail, the information must be sent as a password protected attachment to the e-mail. DHHS Divisions and Offices are discouraged from using direct identifiers in the attached document (e.g., client name, social security number, address) and should de-identify the information whenever feasible.
  - In accordance with the State of North Carolina (NC) Enterprise Security Standard, S002, passwords shall not be inserted into e-mail messages or other forms of electronic communication without proper encryption. Passwords for e-mail attachments shall be provided to recipients in a secured manner (e.g., by phone, fax, or pre-assigned passwords provided to a receiving DHHS Division and Office).
  - Tracking numbers for Incidents should not be sent via email.
  - Ensure that e-mails are addressed correctly by reviewing the recipient's e-mail address before sending the e-mail to ensure that the e-mail software did not automatically fill-in an incorrect e-mail address after the first few characters of the address were typed.
  - When disclosing individually identifying health information to a third party for purposes other than treatment, payment, or health care operations, the disclosure must be documented and accounted for.
  - In the event of a misdirected e-mail with a file attachment that contains individually identifying health information, the recipient must be contacted immediately and shall be asked to delete the e-mail and attachment. Misdirected e-mails are considered accidental disclosures and must be accounted for in accordance with DHHS Privacy Policy, Use and Disclosure Policies, Accounting of Disclosures. In addition, the DHHS Division and Office shall complete a Privacy Incident Report in accordance with DHHS Privacy policies.

  DHHS Divisions and Offices shall include a confidentiality statement on all e-mails containing individually identifiable health information as file attachments.

- **Telephone**

  Whenever it is necessary for staff to discuss individually identifiable health information via the telephone with a client or a client's family members/friends, workforce members, business

associates, other health care providers, or health plans, staff must follow the requirements for protecting such information.

Each DHHS Division and Office shall develop and implement procedures for identifying individuals to whom a specific client's health information may be released via the telephone. Each DHHS Division and Office shall honor any agreed upon requests made by the client as to the use of alternate forms of communication (e.g., alternate telephone numbers) or restrictions regarding the use or disclosure of that clients individually identifying health information. DHHS Division and Office procedures must include the stipulation that telephone conversations that include the use or disclosure of confidential information be conducted in private locations wherever possible and in a soft voice to ensure such information is shared with only the intended recipient.

DHHS Division and Office staff shall not discuss individually identifiable health information (e.g., client's diagnosis or condition) until the following can be confirmed:

- Identity of the caller (e.g., a "call back" to validate the number called or voice recognition) and
- Verification that the caller has a need to know, and the use or disclosure of confidential information is permissible.
- If confirmation cannot be made, the DHHS Division and Office shall neither confirm nor deny that the client has in the past or is currently receiving services from the DHHS Division and Office. The caller's information can be recorded and provided to the client for disposition.

DHHS Division and Office procedures should also include the following practices for making calls:

- DHHS Division and Office staff shall not discuss individually identifiable health information until the identity of the person on the phone line has been confirmed. This may be accomplished through voice recognition or call-back.
- In the event an answering machine/voice mail system picks up the call, staff should leave a message requesting that the person they need to speak to return the call. The message shall include ONLY the name and telephone number of the person that should receive the return call (e.g., "This message is for Mary Jones. Please contact Mary Smith at 555-1313"). Messages left on an automatic answering machine or voice mail system shall not contain confidential health information (e.g., name of the client, diagnosis, test results).

DHHS Division and Office staff shall be informed of the security risks of cellular/wireless phones. Communication via cellular and wireless phones should not be used to discuss confidential information; this communication is not secure, unless encrypted. DHHS Division and Office staff shall not use these devices to communicate confidential information unless there is an emergency and a wired, landline phone is not readily available.

DHHS Divisions and Offices must take reasonable steps to protect the privacy of all verbal exchanges or discussions of individually identifying health information, regardless of where the discussion occurs. Where possible, each DHHS Division and Office shall make enclosed offices and/or interview rooms available for the verbal exchange of individually identifying health information.

In work environments that contain few offices or closed rooms, DHHS staff participating in the verbal exchanges of individually identifying health information shall conduct these conversations in a soft voice and as far away from others as possible.

Guidance:	• Confidential information that is transmitted by facsimile (fax) machines, e-mail, printers, copiers, and by telephone or other oral means of communication shall be protected from unauthorized use and disclosure. DHHS Divisions and Offices shall address measures to direct the conduct of DHHS Division and Office staff in relation to the protection of individually identifiable health information; and develop and implement appropriate DHHS Division and Office safeguard procedures.
	
	• Authorized Disclosures of Individually Identifiable Health Information. Disclosure of individually identifiable health information is essential to health care providers and health plans for a variety of reasons including treatment, payment of health care services, or health care operations (TPO) purposes. Safeguarding such information requires DHHS Divisions and Offices to ensure the following prior to disclosure:
	  o The disclosure is permitted for TPO;
	  o The disclosure is authorized by the client;
	  o The disclosure does not violate a communication or use and disclosure restriction that the client has requested and the DHHS Division and Office has granted; or
	  o The disclosure is required or permitted by law.
	
	• DHHS Divisions and Offices shall develop and implement procedures that ensure that chosen methods of disclosing individually identifiable health information outside the DHHS Division and Office are safeguarded to protect client confidentiality.

2.4.3 Physical Safeguards

Guidance:	• Areas that use white boards, chalk boards, posters, etc. must be evaluated to ensure individually identifiable health information is not displayed or unintentionally disclosed through these devices. For example, DHHS Divisions and Offices may develop the following procedures:
	  o Post client first name and last initial (or vice versa) on boards.
	  o Cover information identifying clients with a cover sheet.
	  o When a client's record is placed in a bin outside an examination/treatment room, position the record so that the client's name is not visible.
	
	• Biomedical devices such as electrocardiograph machines and medical imaging systems must be safeguarded from unauthorized access if they display memory, connect to another system, or transfer data.
	
	• Each DHHS Division and Office shall maintain documentation of building repairs, workspace modifications, and equipment purchases that are instituted to cure physical safeguard deficiencies. Such records will serve as documentation of due diligence.
	
	• DHHS Divisions and Offices shall ensure that observable individually identifying health information displayed on computer screens is adequately shielded from unauthorized disclosure. DHHS Divisions and Offices shall safeguard individually identifiable health information displayed on computer monitors by:
	  o Relocating the workstation or repositioning the computer monitor so only the authorized user can view it;
	  o Installing polarized screens (also referred to as privacy or security screens) or other computer screen overlay devices that shield information on the screen from persons who are not directly in front of the monitor; and
	  o Clearing information from the computer screen when it is not actually being used, turning off computer when not in use, or by activating a password-protected

screensaver.

- Each DHHS Division and Office shall take reasonable steps to ensure the privacy of client information in treatment areas and other areas in the DHHS Division and Office where visitors, repairmen, vendors, and family members are permitted. General safeguards shall include measures the facility has implemented that protect individually identifiable health information from unauthorized use or disclosure.

- Facility Safeguards include the following:
    - Sign-in Sheets - Ensure sign-in sheets that are viewed by multiple clients do not contain health information and unnecessary identification information
    - Client/Staff Conversations - Establish precautions to prevent conversations regarding client information from being overheard by others. Designate an area away from waiting areas to have conversations involving confidential information. Intercom - Limit information given over an intercom system. For example, do not instruct specific clients to report to a certain testing or procedure area.
    - Treatment Areas - Limit access to treatment areas. Individuals that are not essential workforce members (e.g., clients, family members, drug reps) should be escorted in all treatment areas.
    - Client Records - Assure clients records used in treatment areas are reasonably protected to prevent inadvertent disclosures. For example, place a cover sheet over records sitting on a desk or position a client's record so that the client's name is not visible. Maintain client records in secure area. (e.g., locked office/nursing station, locked file cabinet).

- Visitor Safeguards should include:
    - Sign-in Logs - Ensure sign-in logs are used that record the visitor's name, company, area visited, time in, and time out.
    - Badges - Provide visitors with identification badges.
    - Escort - Establish procedures for when visitors must be escorted within the DHHS Division and Office. Unescorted visitor access should be limited to those areas that do not contain individually identifying health information.

- Each DHHS Division and Office shall establish a process for safely disposing of paper and other materials containing individually identifiable health information in accordance with the DHHS Security Manual. Paper records include, but are not limited to, client records, billing records, and correspondence. Other materials include, but are not limited to, client consumables and non-durable medical equipment such as x-ray films, identification bracelets, identification plates, IV bags, prescription bottles, syringes, diskettes, disk drives, etc. It is recommended that, where practical and when permitted, paper materials containing individually identifiable health information be shredded or burned. All steps in the shredding or burning process shall be protected, including any shred/burn boxes, bins, and bags containing individually identifying health information to be destroyed.

- Allowing DHHS workforce members to remove individually identifying health information from DHHS Division and Office premises for purposes other than treatment or in response to a court order or allowing workforce members to access individually identifiable health information outside of the secured work environment, is strongly discouraged. However, it is recognized that there may be circumstances where work outside of the secured environment. DHHS Divisions and Offices shall develop and implement procedures to ensure the security of confidential information taken outside the secured work environment, including, but not limited to, the following guidelines:
    - Ensure privacy and security of remote work area;
    - Restrict telephone conversations to a private area using a wired, landline phone;
    - Ensure faxed documents are handled according to the guidelines in this policy; and

- Secure confidential information in locked rooms or locking storage containers (e.g., filing cabinets, safes, desk drawers) when not in use.
- Original client medical or financial records in paper format shall never be removed from the DHHS Division and Office responsible for safeguarding the records unless under order of the court or when necessary for treatment purposes (which includes autopsies).

Guidance:

- DHHS Divisions and Offices shall safeguard individually identifiable health information that is generated, received, transmitted and/or maintained throughout each DHHS Division and Office by establishing protections used for equipment/supplies/records/work areas to prevent unauthorized use or disclosure of individually identifiable health information maintained by the DHHS Division and Office.

- A physical safeguards assessment shall be conducted, and the associated documentation maintained by each DHHS Division and Office to demonstrate due diligence in complying with DHHS physical safeguards requirements. The information collected will assist each DHHS Division and Office in determining where physical safeguard deficiencies exist and in identifying the measures necessary to secure the area. DHHS Divisions and Offices shall identify in their procedures the frequency and/or circumstances (e.g., office relocations or DHHS Division and Office reorganizations that result in changes in the security of individually identifiable health information) that would require a review and updated physical safeguards assessment.

- Each DHHS Division and Office shall identify those areas wherein staff routinely maintain, transmit, and receive individually identifiable health information on paper, biomedical equipment, or other non-electronic medium (e.g., prescription bottles, test tubes, specimen vials). DHHS Divisions and Offices must ensure these areas are routinely manned or physically secured as appropriate during business and non-business hours and that such areas are accessed only by authorized staff. Securing confidential information may be as simple as employing locks on file cabinets, safes, and desk drawers or as complex as relocating equipment or an entire work area to a more secure location.

- Each DHHS Division and Office shall develop and implement procedures for limiting physical access to individually identifiable health information maintained throughout the DHHS Division and Office while ensuring that properly authorized access is allowed. Physical security of health information is most vulnerable in the following areas:
  - Client records storage areas;
  - Shared office areas containing faxes, copiers, and printers; and
  - Open work areas or workstations.

2.4.4 Technical Safeguards

Guidance:

- Passwords shall not be included in e-mail messages or unencrypted computer files; nor shall passwords be stored in a location readily accessible to others. DHHS Divisions and Offices shall require staff with access to individually identifiable health information to change their password at least every 90 days or immediately if the security of a password has been jeopardized.

- Additional information regarding password protections can be found in the ITS Statewide Information Security Manual.

- DHHS Divisions and Offices shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each DHHS Division and Office by addressing technical safeguards used for accessing confidential information maintained in computer systems and other electronic media through identification of staff who need access to electronic data and control of access through the use of unique user identifiers and passwords.

- Each DHHS Division and Office shall determine which workforce members, or classes of workforce members based on job responsibility, require access to individually identifiable health information. Privileges shall be established on a "need to know" basis for each user relative to their specific relationship with clients and specified business needs for accessing individually identifiable health information. It will be the responsibility of each DHHS Division and Office to determine the level of individually identifiable health information detail a workforce member can access, such as an entire record, department files, individuals' files, workstation, software applications, electronic data, electronic report files (e.g., X/PTR), etc. The access level of individually identifiable health information granted to an individual shall be the minimum necessary needed to do his/her job.

- DHHS Divisions and Offices shall require its staff to use personal passwords in situations determined appropriate by the DHHS Division and Office. DHHS Divisions and Offices shall develop procedures to ensure passwords are protected and define situations or circumstances when a supervisor or other designated staff may have access to a user's password. In special cases where a user is required to divulge his/her personal password such as for system support, the user shall immediately change the password.

2.5 HIPAA Hybrid Entity Designation

This policy shall assess DHHS Divisions and Offices operations for appropriate designation as a HIPAA Covered Entity or Hybrid Entity as defined by the Health Insurance Portability and Accountability Act (HIPAA) and in compliance with HIPAA Privacy Standards, Security Standards, 45 CFR Parts 160, 45 CFR Parts 164, and components of the American Recovery and Reinvestment Act (ARRA).

Guidelines

DHHS Division and Offices shall be assessed for appropriate designation as a Covered Entity or Hybrid Entity. DHHS Divisions and Offices performing both covered and non-covered functions, shall be designated as a hybrid entity under the HIPAA Privacy and Security Standards. The health care components of the hybrid DHHS Division and Office, including all business associate functions, must comply with all the requirements of the HIPAA Privacy and Security Standards. The non-healthcare components of the hybrid entity are not covered by the HIPAA Privacy Standards.

The following terms shall apply to this policy:

- **Covered Entity-** a health plan, health care clearinghouse, or a health care provider who electronically transmits any protected health information (PHI) in connection with transactions that include medical, billing payment, or insurance coverage for which HHS has adopted standards.
- **Hybrid Entity-** a single legal entity that is a covered entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule.
- **Protected Health Information (PHI)-** Any individually identifiable health information, including genetic information and demographic information, collected from an individual that is created or received by a covered entity.
- **Healthcare Component-** DHHS Divisions and Offices that operate as a healthcare plan, a healthcare provider, or healthcare clearing house that use, create, or disclose protected health information (PHI).

2.5.1 Initial Coverage Determination

The initial coverage determination will be scheduled with the PSO Coordinator, the DHHS Division and Office designated Privacy Officer or Security Officer. The determination shall be documented and retained for (six) 6 years.

2.5.2 Subsequent Coverage Determination Notification

Subsequent coverage determination notification shall be initiated by the DHHS Division and Office. On the anniversary month of the prior coverage determination assessment, the DHHS Division and Office shall review their internal operations and notify the PSO Coordinator of the following:

- Annual documentation of new programs or processes that could change the determination from Non-Covered Entity to Hybrid Entity,
- Annual documentation of new programs or processes that could change the determination from Hybrid Entity to Non-Covered entity,
- Annual documentation of "No Change in Status" if applicable.

The DHHS Division and Office shall submit the form titled "Program/Section Change for Hybrid Entity Determination" to notify the PSO office of any new program or section.

The PSO office shall retain all documentation provided by DHHS Divisions and Offices that have complied with notification requirements. DHHS Divisions and Offices that have not notified the PSO coordinator will be contacted and given 30 days to respond with status updates. DHHS Divisions and Offices that report any changes will be contacted to complete the formal coverage determination questionnaire.

2.5.3 Segregation of Functions

DHHS Divisions and Offices must segregate all healthcare components from the non-healthcare components and ensure the following;

- Where possible, staff and office space should be segregated. Where staff are not segregated, the staff must not use or disclose protected health information (PHI) created or received during their work for the health care component in a manner prohibited by the Privacy Standards;
- Reasonably ensure information collected by the non-healthcare component is not filed or electronically intermingled with the designated record set;
- Reasonably ensure information collected by the health care component is not filed or electronically intermingled with information collected during non-healthcare functions. If the information is intermingled, PHI must never be accessed by the non-healthcare component;
- Ensure information is not shared between the healthcare component and the non-healthcare component without a Memorandum of Agreement/Understanding (MOA/MOU).

Chapter 3: HIPAA Use and Disclosure Policies

3.1 HIPAA Use and Disclosures

The final Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule controls the use and disclosure of individually identifiable health information. Generally, covered health care components may not use or disclose individually identifiable health information except in ways identified in the Privacy Rule or when required or allowed by other federal or state laws. All other uses are prohibited, and barriers must be established to prevent any use and disclosure other than those permitted. 'Use' and 'disclosure' are significant terms that distinguish sharing of information within a DHHS Division and Office (use) from releasing information outside an DHHS Division and Office (disclosure).

DHHS Divisions and Offices may not use or disclose individually identifiable health information except either:

- As this policy permits or requires; or
- As the individual who is the subject of the information authorizes in writing.

Throughout this policy whenever a 'client' is addressed, the client's 'personal representative' (including a guardian) shall be treated the same as the client, when the client is unable to act for him/herself.

Guidelines

In accordance with HIPAA, DHHS Divisions and Offices shall disclose individually identifiable health information in the following situations:

- To clients specifically when they request access to their health information (although there are exceptions that are identified in this policy), or when they request an accounting of disclosures of their health information; and
- To the Secretary of the United States (US) Department of Health and Human Services (HHS) when undertaking a compliance investigation, review, or enforcement action.

3.1.1 Permitted Uses and Disclosures

HIPAA permits DHHS Divisions and Offices to use and disclosure individually identifiable health information, as defined by HIPAA, without a client's written authorization under the following circumstances:

- To a client (except as required for access and accounting of disclosures);
- Treatment, payment and health care operations (exceptions for DPH and MH/DD/SAS DHHS Divisions and Offices. Incidental to an otherwise permitted use and disclosure;
- Limited data set [for research, public health, or health care operations);
- Facility directories (unless a client opts out of the directory);
- Notification/involvement with family/others;
- Disaster relief;
- Required by law;
- Public Health activities;
- Abuse and neglect;
- Health oversight activities;
- Judicial and administrative proceedings;
- Law enforcement purposes;
- To avert serious threat to health/safety;
- Specialized government functions;
- Workers' Compensation; and
- Research with Institutional Review Board (IRB) approval (see DHHS Privacy Policy Use and Disclosure Policies, Research).

DHHS Divisions and Offices must rely on professional ethics and best judgment when deciding which of these permissive uses and disclosures to make.

3.1.2 Permitted Uses and Disclosures with Client Authorization

DHHS Divisions and Offices may use and disclose individually identifiable health information <u>only with a</u> <u>client's authorization</u> for the following purposes or situations:

- To anyone, for any reason, that is not for treatment, payment, or health care operations; or otherwise permitted or required by state or federal law/regulation;
- If the individually identifiable health information to be used or disclosed is psychotherapy notes; and
- DHHS Divisions and Offices must make reasonable efforts to use, disclose, and request only the minimum amount of individually identifiable health information needed to accomplish the intended purpose of the use, disclosure, or request for information, except for the following circumstances:
- Disclosure to or a request by a health care provider for treatment purposes;
- Disclosure to a client who is the subject of the information;
- Use or disclosure made pursuant to an authorization;
- Disclosure to HHS for complaint investigation, compliance review, or enforcement;
- Use or disclosure that is required by law; or
- Use or disclosure required for compliance with other HIPAA rules.

Clients may request DHHS Divisions and Offices to restrict all or a portion of their individually identifiable health information from specific uses or disclosures. DHHS Divisions and Offices that have agreed to such restrictions are required to use and disclose the restricted information only as agreed.

DHHS Divisions and Offices that have created information that is not individually identifiable do not have to comply with the use and disclosure requirements, provided that:

- Disclosure of a code or other means of de-identification that can be used to re-identify the client, constitutes disclosure of individually identifiable health information; and
- If de-identified health information is re-identified, DHHS Divisions and Offices must use or disclose such re-identified information only in accordance with the use and disclosure requirements in this policy Disclosures to Business Associates.

3.1.3 Business Associate Disclosures

DHHS Divisions and Offices may disclose individually identifiable health information of clients to a business associate and may allow a business associate to create or receive a client's individually identifiable health information on its behalf [see DHHS Privacy Policy Administrative Policies, Business Associates (Internal/External)].

3.1.4 Deceased Client

DHHS Divisions and Offices must use and disclose individually identifiable health information of a deceased client in the same manner as if the client were still alive. Under the HIPAA Omnibus rule, a decedent's PHI only need be protected for a period of fifty years.

3.1.5 Personal Representative Disclosures

DHHS Divisions and Offices must use and disclose individually identifiable health information to a personal representative of a client in the same way as the DHHS Division and Office would to the client, with two exceptions:

- If the client is an un-emancipated minor (under specific circumstances); and
- In abuse, neglect, and endangerment situations.

3.1.6 Confidential Communications

DHHS Divisions and Offices must make reasonable efforts to comply with requests from clients to disclose confidential communications by alternative means or methods.

3.1.7 Disclosures by Whistleblowers and Workforce Member Crime Victims

DHHS Divisions and Offices shall not be considered in violation of use and disclosure regulations if a member of its workforce or its business associate discloses individually identifiable health information "in good faith" to a health oversight agency or attorney retained by or on behalf of the individual; or if individually identifiable health information is disclosed to law enforcement by a workforce member who is a victim of crime, abuse, neglect, or domestic violence.

Client rights provided by the HIPAA Privacy Rule require DHHS Divisions and Offices to disclose individually identifiable health information to the client who is the subject of the information, unless an agency has a compelling reason not to do so.

3.1.8 HIPAA Use and Disclosures Treatment, Payment, and Health Care Operations

- **Treatment Purposes**

Individually identifiable health information may be used (i.e., shared among designated staff) within a covered health care component to carry out treatment activities. DHHS Divisions and Offices may use a client's individually identifiable health information for its own treatment purposes, including coordination and management of health care services for clients in addition to the following:

  - Use of individually identifiable health information by the workforce within a DHHS Division and Office for treatment purposes does not require written authorization from the client.
  - Use of individually identifiable health information by the workforce for treatment purposes is not subject to the minimum necessary requirements.
  - Use of individually identifiable health information by the workforce for treatment purposes is not required to be accounted for in the DHHS Division and Office Accounting of Disclosures log.
  - Use of psychotherapy notes requires a written authorization from the client who is the subject of the notes.

Guidance:

- **DMH/DD/SAS One Client/One Record**
  Facilities within the Division of Mental Health, Developmental Disabilities and Substance Abuse Services (DMH/DD/SAS) shall share one client record for all treatment services rendered to each individual client within all Division facilities to coordinate treatment, payment, etc. The facility Consent for TPO allows the client record to be "used for treatment purposes" within all the Division facilities. (The DMH/DD/SAS Client Records Manual for State Facilities, APSM 45-3 should be consulted in determining the procedures for sharing one health record per client.)

- **Corporate Master Person Index**
  Facilities within Division of Mental Health, Developmental Disabilities, and Substance Abuse Services are required to furnish individually identifiable health information to the Department for the purpose of maintaining a database of clients served in the state facilities. State facilities may access this database only if such information is necessary for the appropriate and effective evaluation, care, and treatment of a client.

- **Care Coordination**
  Individually identifiable health information may be disclosed (e.g., shared with other health care providers or human service agencies) outside a covered health care component to carry out treatment coordination and management between providers and for referrals to other health care providers for treatment purposes. The following disclosure guidance shall be considered:
  - Disclosure of individually identifiable health information by the workforce in an DHHS Division and Office for treatment purposes does not require written authorization from the client.
  - Disclosures of individually identifiable health information by the workforce in an DHHS Division and Office to another health care provider for treatment purposes are not subject to the minimum necessary requirements.
  - Disclosures of individually identifiable health information for treatment purposes are not required to be accounted for in the Accounting of Disclosures log.

- **Payment Purposes**

Use: Individually identifiable health information may be used (i.e., shared among designated staff) within a covered health care component for payment purposes such as determining or fulfilling the DHHS Division and Office responsibility for coverage and provision of benefits under a health plan; or to obtain or provide reimbursement for the provision of health care. The following use guidance shall be considered:

- Use of individually identifiable health information by the workforce within an DHHS Division and Office for payment purposes does not require written consent from a client.
- Use of individually identifiable health information by the workforce within an DHHS Division and Office for payment purposes is subject to the minimum necessary requirement.
- Use of individually identifiable health information by the workforce within an DHHS Division and Office for payment purposes is not required to be accounted for in the Accounting of Disclosures log.

Disclosure: Individually identifiable health information may be disclosed (e.g., shared with other payers, health care providers, or business associates) outside a covered health care component to carry out payment functions such as eligibility, billing, claims adjustment, and other collection activities. The following disclosure guidance shall be considered:

- Disclosure of individually identifiable health information by the workforce outside the DHHS Division and Office for payment purposes does not require written authorization from the client.
- Disclosure of individually identifiable health information by the workforce in an DHHS Division and Office for payment purposes are subject to the minimum necessary requirements.
- Disclosure of individually identifiable health information by the workforce in an DHHS Division and Office for payment purposes are not required to be accounted for in the Accounting of Disclosures log.

- **Health Care Operations**

Use: Individually identifiable health information may be used (i.e., shared among designated staff) within a covered health care component for health care operation purposes such as conducting quality assessment and improvement activities, business planning and development, business management and administrative activities, student training, and credentialing. The following use guidance shall be considered:

- Use of individually identifiable health information by the workforce within an DHHS Division and Office for health care operation purposes does not require written consent from the client.
- Use of individually identifiable health information by the workforce for health care operation purposes is subject to the minimum necessary requirements.
- Use of individually identifiable health information by the workforce for health care operation purposes is not required to be accounted for in the Accounting of Disclosures log.

Disclosure: Individually identifiable health information may be disclosed (i.e., shared with entities) outside a covered health care component to carry out health care operation functions such as accreditation, licensure, conducting or arranging for medical review, auditing, or legal services that are necessary to run the DHHS Division and Office and to support the core functions of health care treatment and payment. The following disclosure guidance shall be considered:

- Disclosure of individually identifiable health information by the workforce in an DHHS Division and Office for health care operation purposes does not require written authorization from the client.
- Disclosure of individually identifiable health information by the workforce in an DHHS Division and Office for health care operation purposes is subject to the minimum necessary requirements.
- Disclosure of individually identifiable health information for health care operation purposes is not required to be accounted for in the Accounting of Disclosures log.

3.1.9 Use and Disclosures Requiring An Individual Opportunity to Agree or Object

DHHS Divisions and Offices may use or disclose individually identifiable health information in certain circumstances; however they must allow clients the opportunity to agree, object, or restrict certain uses or disclosures of their individually identifiable health information, in advance of the DHHS Division and Office's use or disclosure. Such information must be documented in the client's health record. The following guidance shall be considered:

- Written authorization from a client is not required for such disclosure.
- Oral agreement or objection by a client is acceptable.
- Disclosures for which a client must have an opportunity to agree or object are subject to the minimum necessary requirements.
- Disclosures for which a client must have an opportunity to agree or object are not required to be accounted for in the DHHS Division and Office's Accounting of Disclosures log.

The following circumstances require that the client is provided with the opportunity to agree or object to the use or disclosure of their individually identifiable health information:

- Facility directory/emergency situations;
- Notification or involvement of family member, other relative, or close friend of a client in the client's care or payment related to the client's health care; and
- Disaster relief purposes.

Guidance:

- **Facility directory/emergency situations;**
  DHHS facilities may use the following individually identifiable health information to maintain a directory of facility clients:
  - Client name;
  - Client location in facility;
  - Client condition (in general terms such as good, fair, poor); and
  - Client's religious affiliation.

- **Notification/Involvement with Family/Others**
  In situations where individually identifiable health information of a client is being disclosed to a family member, other relative, or close personal friend of the client **and the client is present**, the DHHS Division and Office must obtain the client's agreement, provide the client with an opportunity to agree or object to the disclosure, or determine, based on the circumstances and

using professional judgment, that the client would not object prior to the disclosure. **If the client is not present** or is incapacitated and cannot agree or object, the DHHS Division and Office must use professional judgment to determine what is in the best interest of the client. In such instances, disclosures must be limited to the information which is directly relevant to the situation.

- **Note:** *Chapter 122C of the NC General Statutes define specific circumstances and conditions when confidential information can be disclosed to family/others by MH/DD/SAS facilities. These facilities shall develop procedures consistent with NC state law.*

3.1.10 Disaster Relief

Use or disclosure of individually identifiable health information for disaster relief purposes (e.g., flood, hurricane, terrorism) must be determined based on professional judgment, taking into account the best interest of the client, and the determination that the requirements do not interfere with the ability to respond to the emergency circumstances.

DHHS Divisions and Offices may use or disclose individually identifiable health information without written authorization and without an opportunity for the client to agree, object, or restrict certain uses or disclosures of their individually identifiable health information in specific circumstances.

3.1.11 Required by Law

DHHS Divisions and Offices may use and disclose individually identifiable health information to the extent that such use or disclosure is required by law, and the use or disclosure complies with and is limited to the relevant requirements of such law. Legal mandates requiring use or disclosure of individually identifying health information may be based upon federal or state statutes/regulations, board of health rules, court orders, and subpoenas issued by a court or other similar judicial or administrative body. Examples of uses or disclosures required by law include the following:

- The Chief Medical Examiner or a county medical examiner may demand the records of a patient who has died and whose death is under investigation (NCGS 130A-385).
- Local health directors or the State Health Director may demand medical records pertaining to the diagnosis, treatment, or prevention of communicable disease (NCGS 130A-144(b)).
- If a health care provider reports an event that may indicate an illness, condition, or health hazard caused by terrorism to a local health director or the State Health Director, the Physicians must report known or suspected cases or outbreaks of reportable communicable diseases to the local health department (NCGS 130A-135).
- Physicians, local health departments, and DHHS shall, upon request and without consent, release immunization information to schools (public, private, or religious), licensed and registered childcare facilities, Head Start, colleges and universities, health maintenance organizations, and other state and local health departments outside North Carolina [NCGS 130A and 10A NC Administrative Code (AC) 41A].
- Health care providers and administrators of health care facilities must report the following types of wounds/injuries to law enforcement authorities: wounds and injuries caused by firearms; illnesses caused by poisoning; wounds and injuries caused by knives or other sharp instruments if it appears to the treating physician that a criminal act was involved; any other wound, injury, or illness involving grave bodily harm if it appears to the treating physician that criminal violence was involved (NCGS 90-21.20).
- All health care facilities and health care providers must report diagnoses of cancer to the central cancer registry (NCGS 130A-209).
- State statutes require all live births, fetal deaths, and deaths, including required medical information related to births and medical certification of the cause of death, to be reported to the local registrar in the county where the birth or death occurred. Physicians, hospitals, medical facilities, birthing facilities, funeral directors, medical examiners, and others as specified are required to provide this information (NCGS 130A-90 - 130A-123).

Note: *Reports made to newspapers or other media regarding birth and/or death announcements require authorization.*

3.1.12 Public Health Activities

There are specific laws that **require** information related to public health activities to be disclosed so those laws would fall under the "required by law" provisions noted in the corresponding section above. There are also some laws that **permit** information related to public health activities to be used or disclosed. DHHS Divisions and Offices may disclose individually identifiable health information related to public health activities to a public health authority when such uses or disclosures are permitted under the law for:

- Prevention and control of disease, injury, and disability. Examples of uses or disclosures permitted for public health purposes for the "prevention and control of disease, injury, and disability; and communicable disease notification" include the following:
  - Health care providers are permitted to report any event that may indicate an illness, condition, or health hazard caused by terrorism to local health directors or the State Health Director (NCGS 130A-476).
  - Medical facilities are permitted to report certain communicable diseases to the local health director (NCGS 130A-137).
  - Hospitals and urgent care centers are permitted to participate in a program for reporting emergency department data to a program established by the State Health Director for public health surveillance purposes (NCGS 130A-476).
  - The State Center for Health Statistics is permitted to collect health data for various health-related research purposes on a voluntary basis – they cannot compel mandatory reporting (NCGS 130A-373).
- Communicable disease notification;
- Child abuse and neglect reporting;
- FDA-regulated product or activity monitoring; and
- Work-related illness or injury monitoring and workplace medical surveillance.

Public health authorities may include the following organizations and individuals:

- Federal: Components and officials of HHS including those within the Centers for Disease Control and Prevention (CDC) and the FDA. The American Association of Poison Control Centers is acting under a cooperative agreement with the CDC to conduct the toxic exposure surveillance system, thus is functioning as a public health authority.
- State: Components and officials of NC DHHS (Division of Public Health), the NC Department of Environment and Natural Resources (DENR), and the NC Department of Agriculture, as well as parallel agencies in other states.
- Local: Components and officials of local health departments and boards of health. Other non-traditional public health authorities might include a county sheriff's office or a private, non-profit organization that is responsible for animal control activities such as rabies control. For child abuse and neglect reporting, the county departments of social services.
- Other: An organization performing public health functions under a grant of authority from or contract with a public health agency [45 Code of Federal Regulations (CFR) 164.501] such as universities, community-based organizations, and others, who in these situations are considered public health authorities when performing public health activities.
- Foreign Government Agencies: In addition to public health authorities, DHHS Divisions and Offices may also disclose individually identifiable health information to an official of a foreign government agency that is acting in collaboration with a public health authority if the public health authority directs the Department to make such disclosure. For example, if the CDC is collaborating with public health officials in Canada while investigating a disease outbreak, a DHHS Division and Office could disclose protected health information to a Canadian government agency if directed to do so by the CDC.

Guidance:

- **Public Health disclosure** procedures include the following:
  - Written authorization from the client is not required.
  - Disclosures are subject to the minimum necessary requirements, unless the law specifies otherwise.
  - Disclosures are required to be accounted for in the DHHS Division and Office's Accounting of Disclosures log.

3.1.13 Communicable Disease Notification

DHHS Divisions and Offices shall disclose individually identifiable health information regarding a client(s) who has been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, according to requirements set forth in Chapter 130A of the NC General Statutes (NCGS).

3.1.14 Child Abuse and Neglect Reporting

Under North Carolina law, any person or institution who has cause to suspect that any juvenile is abused, neglected, or dependent, or has died as the result of maltreatment must make a report to the department of social services in the county where the child lives or is found (NCGS 7B-301).

3.1.15 FDA-Regulated Product or Activity Monitoring

DHHS Divisions and Offices must disclose individually identifiable health information to the FDA when required to do so as related to the quality, safety, or effectiveness of such FDA-regulated products or activities. DHHS Divisions and Offices must ensure staff are aware of such requirements and shall develop a process for ensuring the reporting is handled according to agency requirements. Staff must be knowledgeable of such requirement and assured that the disclosure is not in violation of the DHHS Division and Office's privacy policies and procedures.

DHHS Divisions and Offices may use or disclose individually identifying health information to:

- Collect and report adverse events that are subject to the jurisdiction of the Food and Drug Administration (FDA) as related to the quality, safety, or effectiveness of such FDA regulated products or activities;
- Enable product recalls, repairs, and replacements; and
- Conduct post-marketing surveillance.

3.1.16 Work-related Illness or Injury Monitoring and Workplace Medical Surveillance

DHHS Divisions and Offices may disclose individually identifiable health information to an employer about a client who is a member of the employer's workforce if the employer has requested the DHHS Division and Office conduct an evaluation relating to medical surveillance of the workplace or to evaluate the client for a work-related illness or injury. Information disclosed shall be limited to the work-related illness or injury of the client or to carry out its responsibilities for workplace medical surveillance

DHHS physicians, medical facilities, and laboratories are required to report to the Department all cases of specified serious and preventable occupational injuries that occur while working on a farm, as well as specified serious and preventable occupational diseases and illnesses which result from exposure to a health hazard in the workplace. DHHS Divisions and Offices shall ensure procedures are in place to report required injuries, diseases, and illnesses.

DHHS Divisions and Offices shall develop procedures regarding disclosures for "public health activities that may be made to an employer" about an individual who is a member of the employer's workforce or an individual who is receiving health care at the request of the employer in the following circumstances:

- To conduct an evaluation relating to medical surveillance of the workplace, or
- To evaluate whether the individual has a work-related illness or injury.

The individually identifiable health information disclosed must directly relate to the above circumstances. DHHS Divisions and Offices must provide the individual with a written notice that such information is disclosed to an employer, for public health activity purposes.

3.1.17 Adult Abuse and/or Neglect Reporting

Under North Carolina law (Article 6, Chapter 108A), any person having reasonable cause to believe that a disabled adult needs protective services must make a report to the director of social services. In making such disclosures, staff shall promptly inform the client, in the exercise of professional judgment, that such a report has been or will be made, except if a qualified professional believes informing the client would place the client at risk of serious harm; or if it is determined by staff that informing a client's personal representative would not be in the best interest of the client.

Guidance:	• **Adult abuse and/or neglect reporting** procedures include the following:
	  o Written authorization from the client is not required.
	  o Individually identifiable health information disclosed for such purposes is not subject to the minimum necessary requirements, but professional judgment should be exercised in determining the information that is necessary to meet the purpose.
	  o Such disclosures are required to be accounted for in the DHHS Division and Office's Accounting of Disclosures log.

3.1.18 Health Oversight Activities

DHHS Divisions and Offices may disclose individually identifiable health information to a health oversight agency for health oversight activities authorized by law, including audits, investigations, inspections, licensure, or disciplinary actions, legal proceedings or actions, or other activities necessary for appropriate oversight of:

- The health care system;
- Eligibility programs;
- Compliance with program standards or civil rights laws.
  - **Exception:** Investigation or other activity in which the client is the subject of the investigation or activity that is not directly related to the client's health care, claim for benefits or receipt of public services is not considered a health oversight activity.

The HIPAA Privacy Rule requires the disclose individually identifiable health information to the HHS Secretary, when requested, to determine compliance with the HIPAA Privacy Rule. DHHS Divisions and Offices are required to maintain proper records, and upon request of HHS, to submit compliance reports in such time and manner as determined by the HHS Secretary.

During an investigation or compliance review, DHHS Divisions and Offices must cooperate with HHS. The DHHS Privacy Officer shall be notified of such investigation or compliance review. The following guidelines shall be met:

- Access shall be permitted to HHS during normal business hours to its facilities, books, records, accounts, and other sources of information, including individually identifiable health information, that are pertinent to ascertaining compliance with the requirements or investigation of a complaint;
- If HHS determines that serious circumstances exist, access must be permitted by HHS at any time and without notice;
- If any information required of DHHS Divisions and Offices is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, DHHS Divisions and Offices must so certify and set forth what efforts it has made to obtain the information.

Variations in requirements specific to disclosure to the Secretary of US HHS include the following:

- Written authorization from the client is not required for such disclosures;
- Disclosures to HHS are not subject to the minimum necessary requirements;
- Disclosures to HHS are required to be accounted for in the DHHS Division and Office's Accounting of Disclosures log.

DHHS Divisions and Offices shall use and disclose individually identifiable health information without client authorization only as permitted or required in this policy, or as required by other federal or state laws and regulations. Whenever North Carolina General Statutes and other federal regulations are more stringent than the HIPAA privacy rules, the more stringent requirement prevails.

Although client authorization is not required by law or regulation in the following circumstances, each DHHS Division and Office should exercise professional judgment in determining whether to seek client involvement when using or disclosing that client's confidential information.

Guidance:	• **Health Oversight Activities disclosure procedure include the following:**
	  o Written authorization from the client is not required.
	  o Disclosures are not subject to the minimum necessary requirements.
	  o Disclosures are required to be accounted for in the DHHS Division and Office Accounting of Disclosures log unless the health oversight activity is considered a health care operation. Health care operations may include accreditation, certification, peer review, licensing, or credentialing activities; conducting or arranging for medical reviews (e.g., death reviews); legal services; auditing functions, including fraud and abuse detection and compliance programs; and resolution of internal grievances.

3.1.19 Judicial and Administrative Proceedings

DHHS Divisions and Offices may disclose individually identifiable health information for judicial or administrative proceedings, as required by NC General Statutes, when the use or disclosure is made in response to a(n):

- Court order;
- Administrative tribunal order;
- Subpoena;
- Discovery request; or
- Other lawful purpose.

All disclosures made in judicial and administrative proceedings shall be made only after the identity and authority of any person requesting such disclosure has been verified, and the requisite documentation required for the disclosure has been obtained. A subpoena alone is not enough reason for disclosing confidential information. Both a subpoena and a court order must be issued to compel disclosure.

3.1.20 Law Enforcement Purposes

DHHS Divisions and Offices shall develop procedures that ensure staff is knowledgeable about disclosures that may be made for law enforcement purposes. DHHS Divisions and Offices may disclose individually identifiable health information without client authorization for the following law enforcement purposes when applicable:

- A law which requires disclosure such as reporting of wounds;
  - Court order, court-ordered warrant, subpoena, or summons; Grand Jury subpoena;
- Administrative request including subpoena, summons, or civil or authorized demand; or
- Similar process authorized by law.

A subpoena alone is not enough reason for disclosing confidential information. **Both a subpoena and a court order must be issued to compel disclosure.**

DHHS Divisions and Offices may also disclose limited information for identification and location purposes when requested by a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. Only the following information may be disclosed:

- Name and address;
- Date and place of birth;
- Social Security Number;
- ABO blood type and Rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of physical characteristics.

Note: *There may be federal or state laws that are more restrictive than the requirements in this policy in which case the more restrictive would apply.*

Guidance:

- **Victims of a Crime**

DHHS Divisions and Offices may disclose individually identifiable health information in response to a law enforcement official's request for such information about a client who is, or is suspected to be, a victim of a crime if:

  - The client agrees to the disclosure; or
  - The DHHS Division and Office is unable to obtain the client's agreement because of incapacity or other emergency circumstances, provided that:
    - A violation has occurred;
    - Enforcement activity would be adversely affected if delayed; and • Disclosure is in the best interest of the client.

- **Crime on Premises**

DHHS Divisions and Offices may disclose individually identifiable health information to a law enforcement official when there is belief that a crime (or threat of crime) has been committed on the premises or against staff. However, information disclosed must be limited to the circumstances and client status, including last known name and address**.**

- **Reporting Crime in Emergencies**

If staff in a DHHS Division and Office provides emergency health care in response to a medical emergency off site, the disclose of individually identifiable health information to law enforcement officials if such disclosure appears necessary to alert law enforcement to:

  - The commission and nature of a crime;
  - The location and the victim of such crime; and
  - The identity, description, and perpetrator of such crime.

If the DHHS Division and Office believes that the medical emergency off site is the result of abuse or neglect of the individual in need of emergency health care, they must first use professional judgment to determine if disclosure of individually identifiable health information is in the best interest of the individual.

- **Avert Serious Threat to Health or Safety**

DHHS Divisions and Offices may use and disclose individually identifiable health information to avert a serious threat to health and safety whenever such use or disclosure is consistent with laws and ethical standards and believes it is necessary to:

  - Prevent or lessen a serious and imminent threat to the health or safety of a person or to the public, and the disclosure is to a person or entity that may reasonably be able to prevent or lessen the threat; or
  - Assist law enforcement to identify or apprehend an individual:
    - Where it appears from all the circumstances that the client has escaped from a correctional institution or from lawful custody; or
    - Because of a statement by a client admitting participation in a violent crime that the DHHS Division and Office reasonably believes may have caused serious physical harm to the victim.

Note: *Disclosure is NOT permitted if the DHHS Division and Office learned such information when treating, counseling, or providing therapy for such criminal conduct; or if the client requested to be referred for treatment, counseling, or therapy for such criminal conduct.*

Information disclosed shall be limited to the client's statement and the following identifying information:

  - Name and address;
  - Date and place of birth;
  - Social Security number;

- ABO blood type and Rh factor;
- Type of injury (if applicable);
- Date and time of treatment;
- Date and time of death (if applicable); and
- A description of distinguishing physical characteristics.

- **Law enforcement disclosure** purposes include the following:
  - Written authorization from the client is not required.
    - **Exception:** Individually identifiable health information related to DNA; dental records; or typing, samples, or analysis of body fluids or tissue **may not be disclosed without client authorization**.
  - Disclosures are subject to the minimum necessary requirements, unless the law (including court orders) specifies otherwise.

Disclosures are required to be accounted for in the DHHS Division and Office's Accounting of Disclosures log.

3.1.21 Specialized Government Functions

Unless otherwise prohibited by state or federal law, DHHS Divisions and Offices may use or disclose individually identifiable health information for specialized government functions, if the identity of the individual representing such function is verified. Functions include:

- The Red Cross, Armed Forces personnel, or other authorized agents of the Armed Forces, if deemed necessary by appropriate military command;
- Authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities;
- Authorized federal officials for the provision of protecting the US President or foreign heads of state;
- Authorized federal officials for national security, which may include any of the agencies listed below:
  - The Office of the Director of the Central Intelligence Agency (CIA).
  - The Office of the Deputy Director of the CIA.
  - The National Intelligence Council (and other such offices as the Director may designate).
  - The CIA.
  - The National Security Agency.
  - The Defense Intelligence Agency.
  - The National Imagery and Mapping Agency.
  - The National Reconnaissance Office.
  - Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
  - The intelligence elements of the Army, Navy, Air Force, Marine Corps, Federal Bureau of Investigation, Department of the Treasury, and Department of Energy.
  - The Bureau of Intelligence and Research of the Department of State.
  - Other elements of any other department or agency as may be designated by the President or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community.
- The Department of State to make medical suitability determinations regarding required security clearance, mandatory service abroad, or for a family to accompany a Foreign Service member abroad;
- A correctional institution or law enforcement official with lawful custody of an inmate if necessary, for the health and safety of such individual, other inmates, officers, or other employees at the correctional institution; and
- Government programs that provide public health benefits and governmental agencies administering such programs.

DHHS Divisions and Offices may use or disclose individually identifiable health information as authorized by, and to the extent necessary to comply with laws relating to workers' compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault.

Guidance:	• **Specialized Government Function disclosure** procedures include the following:
	  o Written authorization from the client is not required.
	  o Disclosures are subject to the minimum necessary requirements, unless the law specifies otherwise.
	  o Disclosures are required to be accounted for in the DHHS Division and Office Accounting of Disclosures log.

3.1.22 Personal Representative

A personal representative is any adult who has decision-making capacity and who is willing to act on behalf of a client regarding the use and disclosure of the client's individually identifiable health information. This would include an individual who has authority, by law or by agreement from the client receiving treatment, to act in the place of the client such as spouse, adult children, parents, legal guardians, or properly appointed agents (e.g., an individual who has been given a medical power of attorney). Procedures must be developed that address when a personal representative is required and the responsibilities of the DHHS Division and Office when communicating with a personal representative. Procedures must also include communication requirements if the client is an un-emancipated minor or if the client has been abused, neglected, or has been in an endangerment situation and there is some question about the personal representative's involvement in the care of the client.

3.1.23 Client Photographs

DHHS Divisions and Offices that take photographs of clients for identification purposes must obtain the client's consent prior to photographing. Photographs of clients may not be displayed in the facility or released outside of the DHHS Division and Office without client authorization. DHHS Divisions and Offices may develop their own consent forms allowing the photograph(s) to be taken, but if there is a need to disclose the photograph(s), authorization must be obtained prior to disclosure.

3.1.24 Psychotherapy Notes

Psychotherapy notes are notations that capture a therapist's impressions about a client and contain details of conversations during a private counseling session or a group, joint, or family counseling session. Such notes are considered the therapist's personal notes and are not maintained in the client's health record but are maintained separately by the therapist.

In most cases, including disclosure to another health care provider for treatment, payment or health care operations, psychotherapy notes can only be released with client authorization. However, authorization for the use or disclosure of psychotherapy notes is not required in the following circumstances:

- For use by the originator for treatment;
- For use in education programs including residency or graduate training programs;
- To defend a legal action brought by a client;
- For purposes of HHS determining compliance with the HIPAA Privacy Rules;
- As otherwise required by law;
- By a health oversight agency for a lawful purpose related to oversight of a psychotherapist;
- To a coroner or medical examiner for the purpose of identifying a deceased client, determining a cause of death, or other duties as required by law; or
- To law enforcement in instances of permissible disclosure related to a serious or imminent threat to the health or safety of a person or the public.

A client's right to request access to his/her health care records does not apply to psychotherapy notes maintained by a psychotherapist. The client's psychotherapist or physician must use professional judgment in determining whether a client should have access to psychotherapy notes.

3.1.25 Verification

DHHS Divisions and Offices must obtain proper identification of all individuals, including clients, prior to allowing access to confidential information. DHHS Divisions and Offices must establish and implement written procedures that are reasonably designed to verify the identity and authority of the requestor where the requestor of the information is not known. Knowledge of a person may take the form of:

- A person known by the DHHS Division and Office;
- A known phone or fax number;
- A known address; or
- A known place of business.

Where documentation, statements, or representations, whether oral or written, from the individual requesting individually identifiable health information is a condition of disclosure, the DHHS Division and Office must obtain such documentation or representations prior to disclosing the requested information.

When the person requesting individually identifying health information is a public official, or a person acting on behalf of a public official, the following procedures may be followed:

- If the request is made in person, presentation of a DHHS Division and Office identification badge, other official credentials, or other proof of government status is enough.
- If the request is made in writing, the request should be on the appropriate government letterhead.
- If the request is made by a person who is acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of the agency such as contract for services, Memorandum of Understanding, or purchase order, that establishes that the person is acting on behalf of a public official.

Verification of the authority of a public official or a person acting on behalf of a public official may be managed in the following manner:

- A written statement of the legal authority under which the information is requested, or if a written statement would be impracticable, an oral statement of such legal authority; or
- If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

DHHS Divisions and Offices are required to verify the identity of anyone who is acting on behalf of a client or who is assisting in an individual's care before disclosing individually identifying health information. The client must identify anyone whom the client has authorized to receive the client's individually identifiable health information.

3.1.26 Incidental to an Otherwise Permitted Use and Disclosure

Certain incidental uses and disclosures are permitted if they occur as a by-product of another permissible or required use or disclosure. Such use and disclosures must be considered secondary in nature that cannot reasonably be prevented, are limited in nature, and occurs as a result of another use or disclosure that is permitted by the HIPAA Privacy Rule. For example, if a client is in an examining room and overhears a doctor talking to another client about his treatment, this would constitute incidental access to the health information being discussed.

- Incidental use and disclosure is permitted only if the underlying use and disclosure DOES NOT violate the HIPAA Privacy Rule.
- Reasonable safeguards that have taken into account the size of the DHHS Division and Office, the nature of information it holds, any potential risks to clients' privacy, and potential effects on clients' care and treatment must be in place to limit the instances of incidental use and disclosure.
- An incidental disclosure is not an accidental disclosure and does not have to be accounted for in the accounting of disclosures logs.

3.2 Authorizations

In accordance with Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, each DHHS Division and Office shall make reasonable efforts to protect individually identifying health information maintained by that DHHS Division and Office. Therefore, no DHHS Division of Office shall disclose information about any such individual without that individual's explicit authorization, unless for specifically enumerated purposes such as emergency treatment, public health, law enforcement,

audit/oversight purposes, or unless state or federal law allows specific disclosures.

Guidelines

DHHS Division and Office as identified in the Purpose Section of this policy shall disclose individually identifying health information only upon authorization by the client (or personal representative), unless state or federal law allows for specific exceptions. Authorizations obtained or received for disclosure of individually identifiable health information must be consistent with authorization requirements identified in this policy. An authorization ***permits***, but does ***not require***, a DHHS Division and Office to disclose individually identifiable health information. Each DHHS Division and Office must provide a copy of the signed authorization to the client (or personal representative) upon request.

3.2.1 Standard Authorization Format

DHHS Divisions and Offices may add their contact information and form number to the standard form; however, any other alterations to the standard form must have prior approval by the DHHS Privacy Officer. The DHHS Privacy Officer is responsible for the development and maintenance of the DHHS standard authorization form. Each DHHS Division and Office is responsible for printing its own authorization forms.

The DHHS standard authorization form shall contain the core elements listed below. Any authorization form received by a DHHS Division and Office from an agency/individual outside of DHHS shall be honored only if it contains the following elements:

- A specific and meaningful description of the information to be used or disclosed;
- The name or other specific identification of the person or class of persons authorized to make the requested use or disclosure of the information;
- The name or other specific identification of the person or class of persons to whom the use or disclosure can be made;
- A description of each purpose of the requested disclosure (the statement “at the request of the client” is a sufficient description when a client initiates the authorization and does not, or elects not to, provide a statement of the purpose);
- An expiration date or event that relates to the client or the purpose of the use or disclosure. The following statements meet the requirements for an expiration date or an expiration event if the appropriate conditions apply:
    - The statement “end of the research study” or similar language is sufficient if the authorization is for use or disclosure of individually identifying health information for research.
    - The statement “none” or similar language is sufficient if the authorization is for the DHHS Division and Office to use or disclose individually identifying health information for the creation and maintenance of a research database or research repository; and
    - Signature of the client and the date of the signature. If a client’s personal representative signs the authorization form, a description of the personal representative’s authority to act on behalf of the client must also be provided.
- In addition to the required elements, the authorization form must contain statements that inform the client of the following:
    - The client’s right to revoke the authorization, the exceptions to the right to revoke, and a description of how the client may revoke the authorization;
    - The consequences (as identified in the “Conditioning of Authorizations” section of this policy) to the client for refusal to sign the authorization form; and
    - The potential for information to be subject to re disclosure by the recipient and no longer protected by state or federal law.
- An authorization shall be considered invalid if the document has any of the following deficiencies:
    - The expiration date has passed, or the expiration event is known to have occurred;
    - The authorization form is not completely filled out;
    - The authorization form does not contain the core elements of a valid authorization;
    - The authorization is known to have been revoked;
    - Any information recorded on the authorization form is known to be false; or
    - An authorization for psychotherapy notes is combined with a request for disclosure of information other than psychotherapy notes.

Guidance:

- A separate authorization must be obtained for disclosure of the personal notes of a mental health professional that are separated from the rest of a client's record, except as follows:
  - Use by the originator of the psychotherapy notes for treatment purposes;
  - Use or disclosure by a DHHS Division and Office for its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
  - Use or disclosure by the DHHS Division and Office to defend itself in a legal action or other proceeding brought by a client;
  - Investigations by the Secretary of the US Department of Health and Human Services;
  - Use or disclosure required by law;
  - Health oversight activities;
  - Coroners and medical examiners; or
  - Institution review board or Privacy Board approval for waiver of authorization for research purposes.

- Questions regarding the DHHS Division and Office's authority to disclose psychotherapy notes without a valid authorization should be referred to the DHHS Privacy Officer.

- An authorization for disclosure of individually identifiable health information shall not be combined with any other written legal permission from the client (e.g., Consent for Treatment, Assignment of Benefits); however, research studies that include treatment may combine authorizations for the same research study, including consent to participate in the study.

- An authorization for disclosure of psychotherapy notes may not be combined with any other authorization; however, psychotherapy notes that are needed from more than one provider or are disclosed to more than one recipient may be combined.

- DHHS Divisions and Offices may use a single authorization for disclosure to multiple agencies involved in coordination of care.

- An authorization that specifies a condition for the provision of treatment, payment, enrollment in a health plan or eligibility for benefits may not be combined with any other authorization.

- The provision of treatment**,** payment, enrollment in a health plan or eligibility for benefits shall not be conditioned on whether a client signs an authorization form, except as follows:
  - The provision of research-related treatment can be conditioned on a client authorizing the use or disclosure of individually identifiable health information for such research;
  - Provision of health care solely for the purpose of creating individually identifiable health information for disclosure to a third party (e.g., physical exam for life insurance); or
  - Prior to enrollment in a health plan if authorization is for eligibility or enrollment determinations and the authorization is not for disclosure of psychotherapy notes.

3.2.2 Signatures

Guidance:

- Each authorization must be signed and dated by the client (or personal representative). If a client's personal representative signs the authorization form, a description of such authority to act for the client must also be documented on the form.

- In any of the mental health/developmental disabilities/substance abuse services institutions operated under the authority of DHHS, the health information of a competent adult or minor whose legal guardian has consented to treatment is to be disclosed to an external client advocate, the competent adult must sign. In situations wherein the client has been adjudicated incompetent and/or is a minor, then the legally responsible person of such client must sign the authorization.

- In the psychiatric hospitals and alcohol and drug abuse treatment centers operated under the authority of DHHS, when minors are receiving treatment for alcohol or substance abuse, based upon the consent of their personal representative, the minor and personal representative must both sign the authorization.

- G.S. 90-21.5 allows a provider to treat a minor client without consent of a parent or personal representative. When the minor consents to treatment, only the minor is required to sign the authorization.

- Should a client (or personal representative) be unable to sign his/her name, an "x" or other mark/symbol is acceptable in place of a signature, as long as it is witnessed and documented, attesting to the validity of the signature.

3.3.3 Dates

Guidance:

- Each authorization must state an expiration date or event, such as a specific time (e.g., January 1, 2003); a specific time period (e.g., one (1) year from the date of signature); or an event directly relevant to the client or the purpose of the disclosure (e.g., 60 days following discharge from the facility). Unless revoked sooner by the client, an authorization will be valid for a period up to one (1) year, except for financial transactions, wherein the authorization shall be valid indefinitely.

- The expiration date or event for each authorization must be acknowledged and actions taken on that authorization must be consistent with such limitations.

3.3.4 Revocation of Authorization

Guidance:

- The authorization must state that a client has the right to revoke the authorization at any time, except to the extent that the DHHS Division and Office has already taken action based upon the authorization. The department strongly recommends that clients be encouraged to sign a revocation statement that becomes a permanent part of the record. Should a client refuse to sign a request for revocation, the verbal revocation statement should be witnessed by a third-

party and documentation of the request should be placed in the client's record. The authorization form must include instructions on how the client may revoke an authorization.

3.3.5 Retention Period

Guidance:

- DHHS Division and Office that maintains authorization forms in their client records must adhere to the retention period in their retention and disposition schedule for client records.
- If authorization forms are maintained separately from client records, the authorization forms must be maintained in accordance with the *General Schedule for State Agency Records* issued by the North Carolina Department of Cultural Resources, DHHS Division of Archives and History, Archives and Records Section, Government Records Branch.

3.3.6 Photocopy/Facsimile Authorization

Guidance:

- An original authorization form is preferred for disclosure of individually identifiable health information; however, a clear and legible photocopy/facsimile is acceptable.

3.3.7 Contractor Authorizations

Guidance:

- The authorization requirements contained in this policy also apply to contractors who perform a service for or on behalf of a DHHS Division and Office. Such contractors are limited to those disclosures permitted in an agreement with the DHHS Division and Office. Contractors are responsible for ensuring these policy requirements are enforced with any sub-contractors they may use.

3.3 Consent for Treatment, Payment, and Health Care Operations

The HIPAA Privacy Rule allows covered health care components to use individually identifiable health information within the facility and to disclose individually identifiable health information outside the facility without consent from the client or the client's personal representative for the purposes of treatment, payment, and health care operations. NC General Statue (GS) 122C-52(a) requires written consent for disclosure of confidential information unless there are other state laws that permit such disclosures without consent; therefore, NC law preempts the HIPAA Privacy Rule and consent must be obtained prior to release of individually identifying information.

Guidelines

To ensure compliance with the NC General Statues and other applicable laws, the Department shall follow this policy in the use and disclosure of health information for treatment, payment, and health care operations (TPO).

3.3.1 Consent

The DHHS Consent form for TPO allows staff in DHHS Divisions and Offices to share and use the health information of clients who are receiving treatment in their facility and to disclose individually identifiable information outside the facility for TPO purposes. This consent form shall not replace a Consent for Treatment form or the Authorization to Disclose Health Information form. The following shall apply for valid consent for TPO:

- Signed by the patient or patient representative
- Valid for up to 1 year, after which time a new consent must be completed and signed
- A new Consent form shall be completed when a new person or agency not originally covered in the consent form is identified as a recipient of individually identifiable health information for TPO
- For payment purposes, Consent is valid until the of the disclosure is satisfied

3.3.2 DMH/DD/SAS

Facilities operated by DMH/DD/SAS shall obtain written consent from the client or personal representative prior to use or disclosure of individually identifiable health information for TPO purposes. No covered health care component may condition treatment on the client providing consent for TPO.

3.3.3 Consent Form

DHHS Divisions and Offices shall provide a template for use by all facilities in developing their consent forms and using and/or disclosing individually identifiable health information for TPO. The consent template shall contain the basic elements required by state and federal laws and regulations. DHHS Divisions and Offices may add additional elements to meet the needs of each facility.

Guidance:

- DHHS and Offices with facilities, must specify the differences in requirements and implementation of:
  - DMH/DD/SAS Consent for TPO,
  - Facility Consent for Treatment,
  - DHHS Authorization to Disclose Health Information
- Each facility shall develop its consent form with elements necessary for that facility and obtain consent upon the time of admission of the client.
- Facilities with long-term patients shall maintain the client consent form in the client record as part of the annual review.
- Facilities must document procedures on when to obtain consent for long-term patients who did not obtain such at the time of admission.
- When no Consent for TPO is obtained from clients already residing in the facility, staff shall disclose information for TPO purposes only as identified in the DHHS Notice of Privacy Practices.

3.3.4 Exceptions

Exceptions to the consent requirement permit use and disclosure without consent as follows:

- Should a client's mental condition be such that it is impossible for the client to understand and sign a consent for TPO, such information must be documented in the client record
- Should a client's mental condition be such that it is impossible for the client to understand and sign a consent for TPO, such information must be documented.
- Should a client be admitted in an emergency, such information must be documented and consent for TPO should be obtained when the client has stabilized.
- Should a client be involuntarily admitted and refuse to sign consent, such information must be documented and signature of the consent for TPO should be attempted at a later date.
- Should there be a substantial communication barrier and the client clearly does not understand the process, such information must be documented and consent for TPO should be obtained when a translator is available to explain the need for consent.
- Should a client understand the request and refuse to sign consent, such information must be documented including the attempt and the reason the client would not sign.

3.4 Minimum Necessary

This policy establishes the requirements for all Department workforce and to protect privacy rights for PHI and PII as required by the Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 and all federal regulations. Department workforce must rely heavily on the development and implementation of policies and procedures. Therefore, this policy takes on special importance for DHHS.

Guidelines

It is each Department workforce member's responsibility related to using and disclosing only the minimum amount of individual identifiable health information (IIHI) and personally identifiable information (PII) to fulfill the purpose of the use or disclosure, regardless of the extent of access provided. This policy covers uses and disclosures of confidential data including PHI and PII in any form including oral, written and/or electronic media. Each workforce member is responsible for adhering to this policy by using only the minimum information necessary to perform his or her responsibilities, regardless of the extent of access provided or available.

Only Department workforce members with a legitimate "need to know" may access, use, or disclose confidential data or PHI. All DHHS Divisions and Offices must make reasonable efforts to limit PHI, IHII, and PII to that which is minimally necessary to accomplish the intended purpose for the use, disclosure, or request for information. This includes all activities related to treatment, payment, and health care operations (TPO). Each workforce member may only access, use, or disclose the minimum information necessary to perform his or her designated role regardless of the extent of access provided to him or her.

3.4.1 Minimum Necessary within NC DHHS

DHHS Divisions and Offices are required to identify persons in its workforce who need access to confidential data including PHI and the categories of information to which access is needed. DHHS Divisions and Offices must develop and implement procedures that limit routine disclosures of PHI, PII, and IIHI to the amount reasonably necessary to achieve the purpose of the disclosure. In addition, DHHS Divisions and Offices are required to develop criteria designed to limit PHI and PII to the minimum necessary standard.

Guidance:

- When using confidential data and PHI internally, DHHS Divisions and Offices must categorize users by their "need-to-know" to accomplish their job responsibilities and establish standard protocol (criteria) that reasonably limits inappropriate access to PII and PHI based on the following categories:
    - Identify the persons or groups of persons who need access to individually identifiable health information to carry out their job functions;
    - Identify the type of individually identifiable health information to which each person or group needs access, as well as the conditions under which they need the access; and
    - Make reasonable efforts to limit the access of its staff to only the information appropriate to their job functions. Standard protocol for disclosures of PHI, PII, and IIHI by an DHHS Division and Office own workforce.

3.4.2 Minimum Necessary Outside NC DHHS

Department workforce members may rely on a request for disclosure as being limited to confidential data (PII and PHI) that is minimally necessary, if:

- Disclosure is to a public official who represents that the request is for the minimum necessary information;
- The request is from another HIPAA covered health care component;
- The request is from a professional in the DHHS Division and Office's own workforce or from a business associate, and the professional represents that the request is for the minimum necessary information; or
- The requestor provides documentation that the disclosure is for research purposes. The minimum necessary requirement **does not** apply to the following:
    - Requests by another HIPAA covered healthcare component;
    - Uses or disclosures made to the individual who is the subject of the PHI;

- Uses or disclosures made pursuant to a HIPAA compliant authorization;
- Disclosures to the Secretary of the Department of Health and Human Services (DHHS) when required by the Secretary to investigate or determine the facility's compliance with the HIPAA Privacy Standards;
- Uses and disclosures required by law as described in §164.512(a); and limited data sets and de-identified information.

Guidance:

- With respect to system access, minimum necessary will be supported through authorization, access, and audit controls (e.g., roles-based access) and should be implemented for all systems that contain confidential data including protected health information (PHI). Within the permitted access, an individual system user is only to access what they need to perform his or her job functions.

- Each DHHS Division and Office must identify workforce members or classes of workforce members who need access to PHI t and PII to carry out their job functions.

- Department workforce may rely on a requested disclosure as being the minimum necessary when:
  - Making disclosures to public officials as permitted in §164.512 if the public official represents the information requested as the minimum necessary;
  - The information requested is requested by a professional who is a member of the DHHS workforce or is a business associate of a DHHS Division and Office for providing professional services to the facility, and the professional represents the information requested as the minimum necessary; and
  - Documentation or representations that comply with the applicable requirements of
  - §164.512(i) have been provided by a person requesting the information for research purposes.

3.4.3 Minimum Necessary for Routine Use or Disclosure

For disclosures and requests made on a routine and recurring basis, the facility must create, implement, and maintain policies and procedures or standard protocols that limit the PHI to the amount reasonably necessary to achieve the purpose of the disclosure.

Guidance:

- For routine recurring disclosures of PHI and PII by DHHS workforce members, standard protocol must:
  - Identify the types of information to be disclosed;
  - Identify the types of persons who would receive such information;
  - Identify the conditions that would apply to such access; and
  - Develop reasonable criteria for disclosures to routinely hired types of business associates (medical transcription, release of information (ROI) vendor, e.g.).

3.4.4 Minimum Necessary for Non-Routine and Other disclosures

For disclosures and requests made on a non-routine basis, criteria must be developed and maintained to limit PHI to the information reasonably necessary to accomplish the purpose of the disclosure and each request must be reviewed on an individual basis in accordance with such criteria.

For **all other requests** for PHI or PII by an DHHS Division and Office's own workforce, standard protocol must ensure that each request is reviewed by a DHHS Division and Office Privacy Official who has authority to determine that the information requested is limited to what is reasonably necessary to accomplish the purpose of the request.

Individuals or entities external to the department that perform activities or functions on behalf of a DHHS covered health care component as defined by the HIPAA Privacy Rule, are considered **External Business Associates** of a DHHS Division and Office. As such, External Business Associates are required to comply with the Minimum Necessary requirement as specified in the HIPAA Privacy Rule.

3.5 De-Identification of Health Information and Limited Data Sets

The purpose of this policy is to define methods by which the DHHS Divisions and Office may remove specific elements from health information so the resulting information will not be considered individually identifying health information. De-identified information can be used or disclosed without employing privacy protections.

In addition to de-identifying health information, HIPAA permits the creation of a "limited data set" that can contain specific individual identifiers when such information is needed for public health, research, or health care operations activities and a "data use agreement" (DUA) has been executed. There are provisions in HIPAA, state laws, and other federal laws when individually identifying health information can be used and disclosed for public health, research, and health care operations without the necessity for a limited data set or data use agreement (e.g., public health disclosures required by law, licensure surveys). Therefore, data use agreements would only be needed for those public health, research, or health care operation uses and disclosures that are not otherwise permitted by federal or state laws.

Guidelines

DHHS Divisions and Offices shall comply with all conditions in this policy regarding the creation, use, and disclosure of health information for which the elements that could reasonably be expected to identify a specific individual have been removed or restricted to a limited data set. Each Office and DHHS Division that is a recipient of a limited data set must sign a data use agreement and shall comply with the conditions of that agreement. A DHHS Division and Office may use the limited data set for its own activities or operations provided that the information used is the minimum necessary to accomplish the intended purpose.

This policy shall apply to *paper* documents as well as *electronic* data in any form (e.g., paper or electronic records, system data, tape, disc, etc.) When information cannot be de-identified or included in a limited data set, the DHHS Division and Office shall ensure that disclosure of the health information is permitted by law and is in accordance with DHHS Privacy Policies.

3.5.1 Protected Health Information Individual Identifiers

For the purposes of DHHS Privacy Policies, the following elements are considered individual identifiers if they apply to DHHS clients or relatives, guardians, employers, or household members of DHHS clients. If the elements below are associated with health information, the information becomes individually identifying health information that must be protected from improper use or disclosure:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes, except for the initial (3) three digits of a zip code if, according to the current publicly available data from the bureau of the census;
- The geographic unit formed by combining all zip codes with the same three (3) initial digits contains more than 20,000 people; and
- The initial three (3) digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security Numbers (SSN);
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;

- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code that can be re-identified

3.5.2 De-Identification

Individually identifiable health information is de-identified when elements have been removed that could identify an individual and there can be no reasonable basis to believe that the information may be used, with or without other available information, to identify an individual. De-identified health information may be used and shared as necessary in the performance of a DHHS Division and Office's work, unless the information is otherwise restricted by federal or state laws.
Such health information may be considered de-identified only if the following criteria are met:

- The DHHS Division and Office is unaware of a means by which the information could be used alone or in combination with other information to identify an individual who is the subject of the information; and a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (e.g., statistician I or II);
- Determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information; and
- Documents the methods and results of the analysis that justify such determination; or
- The identifiers (listed above) of the client or relatives, guardians, employer, or household members of that client are removed.

An DHHS Division and Office may engage a business associate to serve as the qualified person with "appropriate knowledge and experience with generally accepted statistical and scientific principles and methods" to de-identify information.

Note: *Several DHHS divisions, facilities and schools employ individuals with statistical background/experience who may be able to provide this type of service.) The use of the disclosed data and the recipients of the data shall be considered in the risk assessment conducted by the qualified person. An DHHS Division and Office that uses an internal or external person to satisfy this de-identification criteria shall develop a procedure to verify that the individual adequately meets the knowledge and experience criteria.*

Health information that has been considered de-identified does not meet the de-identification criteria if either of the following is true:

- A code or other means of record identification designed to enable coded or otherwise deidentified information to be re-identified is provided; or
- De-identified information is re-identified.

3.5.3 Limited Dataset

DHHS Divisions and Offices may use or disclose individually identifying health information that contains a limited number of identifiers (i.e., *limited data set*) for public health, research, or health care operation activities whenever the limited data set will meet the intended purpose for the use or disclosure. When a limited data set is deemed appropriate for a use or disclosure, DHHS Divisions and Offices will enter into a data use agreement, using a DHHS Data Use Agreement, with the recipient of the information unless the use or disclosure is permitted by state or federal law, which negates the need for such an agreement. When limited data sets are used or disclosed with an appropriate data use agreement executed:

- An authorization is not required for the use or disclosure of a limited data set; and
- Limited data sets do not need to be included in an accounting of disclosures.

To qualify as a limited data set, the following identifiers for DHHS clients or relatives, guardians, employers, or household members of those clients can be associated with health information:

- State, county, city or town, zip code, SSN;
- Birth date, admission date, discharge date, date of death;
- Age; and/or

- Unique identifying number, characteristic, or code exclusive of identifiers such as SSN, account numbers, medical record numbers, etc., as listed in the Exclusion of Data Elements section below.

3.5.4 Exclusion of Data Elements Considered to be Identifying Elements

The table below outlines the identifiers that must be **excluded** from individually identifying health information in order to consider the information as de-identified or as a limited data set. (See Appendix A for a list of all elements that can be **included** in de-identified information or a limited data set.)

DATA ELEMENTS THAT MUST BE EXCLUDED TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET		
ELEMENTS	**DEIDENTIFIED ELEMENTS**	**LIMITED DATA SET ELEMENTS**
Names of clients or employers, household members, guardians, or relatives of clients	X	X
Street address or post office box number of clients or employers, household members, guardians, or relatives of clients	X	X
County, city, town, or precinct of clients or employers, household members, guardians, or relatives of clients	X	
State of clients or employers, household members, guardians, or relatives of clients		
First three (3) digits of the zip code of clients or employers, household members, guardians or relatives of clients **if,** according to the Bureau of Census, **the population of all zip codes with the same first three (3) digits is greater than 20,000 people**. E.g., If the population of all zip codes that begin with 276 is more than 150,000, you can include 276 in de-identified health information.		
First three (3) digits of the five digit zip code of clients or employers, household members, guardians or relatives of clients **if**, according to the Bureau of Census, **the population of the all zip c odes with the first three (3) digits is less than 20,000 people**. E.g., The total population for all zip codes starting with 211 - say 21101 and 21104 - is 19,200 people. In this case, you could not use the first three (3) digits of the zip code in de-identified health information.	X	
Last two (2) digits of the zip code of clients or employers, household members, guardians or relatives of clients	X	

Five (5) digit zip code of clients or employers, household members, guardians, or relatives of clients. E.g., the five (5) digit zip code of 27603 must be excluded from de-identified data but can be included in a limited data set.	X	
Dates exclusive of year (e.g., month/day) directly related to a client including admission date, discharge date, date of death	X	
Birth date exclusive of year (e.g., month/day) for clients age 89 and under	X	
Birth date inclusive of year (e.g., Month/Day/Year) for clients age 90 and above (not aggregated - e.g., 1880-1913)	X	
Age 89 and under		
Specified ages 90 or above (not aggregated - e.g., 90+)	X	
Telephone numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Fax numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Electronic mail addresses of clients or employers, household members, guardians, or relatives of clients	X	X
SSN of clients or employers, household members, guardians, or relatives of clients	X	X
Medical record numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Health plan beneficiary numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Account numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Certificate/license numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Vehicle identifiers and serial numbers, including license plate numbers, of clients or employers, household members, guardians, or relatives of	X	X
clients		

Medical device identifiers and serial numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Web Universal Resource Locators (URLs) of clients or employers, household members, guardians, or relatives of clients	X	X
Internet Protocol (IP) address numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Biometric identifiers, including finger and voice prints of clients or employers, household members, guardians, or relatives of clients	X	X
Full face photographic images and any comparable images of clients or employers, household members, guardians, or relatives of clients	X	X
Any other unique identifying number, characteristic, or code (unless such code is developed in accordance with the *Re-Identification* section of this policy)	X	
Gender, race, ethnicity, or marital status		

3.5.5 Reidentification

An DHHS Division and Office may assign a code or other means of identification to allow information that has been de-identified to be re-identified *within the DHHS Division and Office*, provided that:

- The code or other means of identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual (examples would be codes containing a SSN or the unique ID algorithm assigned to clients served in facilities operated by the DHHS Division of Mental Health, Developmental Disabilities, and Substance Abuse Services);
- The DHHS Division and Office does not use or disclose the code (or other means of identification) for any purpose other than that originally intended; and
- The DHHS Division and Office does not disclose any methods that can be used to re-identify information that has been de-identified.

3.5.6 Data Use Agreement

DHHS Divisions and Offices that use or disclose a limited data set, wherein the use or disclosure is not permitted by state or federal law, the DHHS Division and Office shall enter into a data use agreement with the limited data set recipient(s) consistent with a DHHS Data Use Agreement provided by the department. The data use agreement must contain the following:

- A requirement to use or disclose such information only for the purposes of research, public health, or health care operation activities;
- Specifications regarding who can use or receive the limited data set;
- Specifications of the permitted uses and disclosures;
- A stipulation that the recipient will not use or disclose the limited data set for any purposes other than those specified in the data use agreement or as otherwise required by law;
- Adequate assurances that the recipient will use appropriate safeguards to prevent the use or disclosure of the limited data set for any purposes other than those specified in the data use agreement. These assurances may be addressed through language similar to that provided in a DHHS Data Use Agreement;

- Commitment by the recipient to report to the DHHS Division and Office any use or disclosure of the information not provided for by the data use agreement of which it becomes aware;
- Assurance that any agent, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- A commitment by the recipient that they will not re-identify the information or contact any of the individuals whose data is being disclosed.

If a DHHS Division and Office staff member becomes aware of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the recipient's obligation under the data use agreement, the staff member shall notify that DHHS Division and Office privacy official who shall take reasonable steps to cure the breach or end the violation. If unsuccessful, the DHHS Division and Office privacy official shall ensure that disclosure of limited data sets to the recipient is discontinued. The DHHS Division and Office privacy official shall report the problem to the DHHS Privacy Officer, who will determine if further actions are warranted which could include reporting the material breach to the Secretary of the US Department of Health and Human Services.

The minimum necessary rule shall apply to limited data sets; therefore, only data elements that are necessary to perform the purpose(s) specified in the data use agreement should be included in the limited data set released to the recipient.

Guidance:

- Each DHHS Division and Office shall identify those areas within the Department that may use or disclose health information that includes any of the identifiers specified in this policy for purposes other than treatment or payment or when authorized by the client. Each DHHS Division and Office shall ensure that staff in these areas understand:
    - The elements that constitute identifiers;
    - The potential for use or disclosure of limited data sets when data use agreements are in place; and
    - That there are specific laws that must be adhered to when using or disclosing individually identifying health information.

- A business associate who has entered into an approved Business Associate Agreement with the DHHS Division and Office may be engaged for the purpose of converting individually identifiable health information into de-identified health information or a limited data set.

- Each DHHS Division and Office shall develop a procedure to ensure compliance with this policy regarding deidentified health information and limited data sets. This procedure shall include oversight, which may be centralized and/or may include a committee review, as well as procedures for coding and re-identifying individually identifying health information that are in accordance with the coding requirements in this policy.

- If time constraints prohibit the immediate creation of de-identified health information, these circumstances shall be documented and provided to the DHHS Division and Office privacy official. When practicable, these issues shall be resolved to enable de-identification for future comparable occurrences.

3.5.7 Elements Permitted in De-Identified Health Information and Limited Data Sets

The table below lists the elements that can be included in de-identified health information. The table also identifies those data elements, including some individual identifiers that are allowed to be included in a limited data set. Note that the individual identifiers that are allowed to be included in a limited data se are not likely to identify an individual if not additional individual identifiers are used.

IDENTIFYING DATA ELEMENTS THAT CAN BE INCLUDED IN DE-IDENTIFIED DATA OR A LIMITED DATA SET (`X' indicates that the element can be included)		
ELEMENTS	**DEIDENTIFIED ELEMENTS**	**LIMITED DATA SET ELEMENTS**
ADDRESS		
County, city, town, or precinct of clients or employers, household members, guardians, or relatives of clients		X
State of clients or employers, household members, guardians or relatives of clients.	X	X
First three (3) digits of the zip code of clients or employers, household members, guardians or relatives of clients **if,** according to the Bureau of Census, **the combined population of all zip codes with the same first three (3) digits is greater than 20,000 people**	X	X
First three (3) digits of the five (5) digit zip code of clients or employers, household members, guardians or relatives of clients **if**, according to the Bureau of Census, **the combined population of the all zip codes with the first three (3) digits is less than 20,000 people**		X
Five (5) digit zip code of clients or employers, household members, guardians, or relatives of clients		X
DATES		
Year of client-related dates, including admission date, discharge date, and date of death	X	X
Dates exclusive of year (month/day) directly related to a client, including admission date, discharge date, and date of death		X
Year of birth for clients age 89 and under	X	X
Year of birth for clients age 90 and above		X
Aggregated years of birth for clients age 90 and over (e.g., 1880-1913)	X	X
AGE		
Age 89 and under	X	X
Ages 90 or above (not aggregated - e.g., 90 or 98)		X
Aggregated ages, including ages 90 and over (e.g., 5-15 or 90-105)	X	X
OTHER		
Any other unique identifying number, characteristic, or code (unless such code is developed in accordance with the *Re-Identification* section of this policy) that is **not one of the following:**		X

SSN, Account numbers, IP address numbers, Vehicle IDs/serial, Health Plan Beneficiary number, Medical Record Number, Certificate/license numbers, Telephone number, Medical device IDs/serial numbers, Fax numbers.		
Gender, race, ethnicity, or marital status	X	X

3.6 Research

To provide guidance to DHHS Divisions and Offices on the requirements under HIPAA's definition of research and North Carolina Administrative Code, 1-ANCAC 28A.0102. For the purposes of this policy, this definition of research is expanded for institutions operated by the DHHS Division of Mental Health, Developmental Disabilities and Substance Abuse Services (DMH/DD/SAS) to include the definition of research provided in North Carolina Administrative Code (NCAC), 10A NCAC 28A.0102, in which "'research' means inquiry involving a trial or special observation made under conditions determined by the investigator to confirm or disprove an [sic] hypothesis or to explicate some principle or effect."

The privacy rule also defines the means by which clients will be informed of uses and disclosures of their individually identifying health information for research purposes, and their rights to access their health information held by covered health care components and internal business associates. Where research is concerned, the privacy rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct vital research. The requirements in this policy are in addition to (not a replacement for) other policies and regulations for human subjects research.

Guidelines

DHHS Divisions and Offices conducting research on clients shall have access to an Institutional Review Board established in accordance with the Common Rule (45 CFR 46, Subpart A) that will:

- Review and modify, disapprove, or approve research protocols and informed consent for research forms; and
- Conduct periodic reviews of the research.

DHHS researchers shall request the individually identifying health information that is the minimum necessary to conduct the research. Whenever possible, DHHS researchers shall request either de-identified data or a limited data set as necessary if either of these is the minimum necessary for conducting the research.

Each DHHS researcher that is a recipient of a limited data set shall sign a data use agreement with the DHHS Division and Office that maintains the information and shall comply with the conditions of that agreement, in accordance with the DHHS policies.

Each DHHS researcher that receives individually identifiable health information from a DHHS covered health care component or internal business associate shall ensure that the information is protected in accordance with the DHHS Privacy Policies.

For treatment purposes, DHHS covered health care components shall contact researchers (either internal or external to DHHS) if a research subject seeks additional health care services from or is admitted into the component for additional treatment.

3.6.1 Researchers External to DHHS

DHHS Divisions and Offices that receive requests for individually identifying health information from researchers external to DHHS shall require the researcher to submit the request in writing. Research requests must be documented in accordance with the requirements identified in this policy.

3.6.2 Institutional Review Boards IRB

Institutional Review Boards (IRBs) are responsible for reviewing and modifying (to secure approval), disapproving, or approving the following for research involving human subjects:

- Research protocols;
- Forms to be used by researchers to obtain authorizations for the use or disclosure of client's individually identifying health information for research;
- Forms to be used by researchers to obtain informed consents from research subjects;
- Requests to waive or alter the requirement for client informed consent for participation in research study; and
- Requests to waive or alter the requirement for client authorization for the use or disclosure of client individually identifying health information for research.

DHHS Divisions and Offices conducting research involving human subjects shall either:

- Establish an internal IRB in accordance with the Common Rule as necessary to review, approve, and monitor such research; or
- Identify an IRB external to DHHS that will review, approve, and monitor such research.

DHHS IRBs shall implement and document procedures for normal review as defined in 45 CFR 46.108(b), or expedited review according to the procedures defined by 45 CFR 46.110.

DHHS IRBs shall document all decisions regarding the modification, approval, or disapproval of research protocols, documentation, and requests to waiver or alter the informed consent or authorization requirements. The IRB shall also record meeting minutes and document continuing review activities.

These records shall be maintained for a minimum of three (3) years, as required by 45 CFR 46.115.

3.6.3 Research Conducted with Client Authorization

Unless otherwise permitted by this policy, or required by state or federal law, a client authorization must be obtained prior to the use or disclosure of the subject's individually identifiable health information for research purposes. Any authorization form received by a DHHS Division and Office from a researcher external to DHHS must contain the following elements to be considered valid:

- A specific and meaningful description of the information to be used or disclosed;
- The name of the entity (e.g., Dorothea Dix Hospital) authorized to disclose the individually identifying health information for research purposes;
- The name of the researcher or entity conducting the research to whom the disclosure of individually identifying health information for research purposes can be made;
- A description of the specific research study in which the information will be used
    - (authorizations cannot be used for nonspecific research or future, unspecified projects);
- An expiration date or event (e.g., client discharge) for the authorization that relates to the client or the research. The following statements meet the requirements for an expiration date or an expiration event if the appropriate conditions apply:
    - The statement "end of the research study" or similar language;
    - The statement "none" or similar language if the purpose of the authorized disclosure of individually identifying health information is for the researcher to create and maintain a research database or repository;
    - Signature of the client and the date of the signature. If a client's personal representative signs the authorization form, a description of the personal representative's authority to act on behalf of the client must also be provided.

An authorization is always required for access, disclosure, or use of psychotherapy notes for research purposes. An authorization for access, use, or disclosure of psychotherapy notes for research may not be combined with any other authorization except other authorization for access, disclosure, or use of the same notes. DHHS Divisions and Offices shall provide a copy of the signed research authorization to clients or their personal representatives.

If a client elects to revoke his/her authorization for the use and disclosure of individually identifying health information for research purposes, the revocation must be documented on the original authorization form in the Revocation section. This revocation shall become a permanent part of the research record and the client's medical record. Researchers within DHHS shall report the revocations to the institutional review board at the time of continuing review.

Note: *Client authorization for use and disclosure of individually identifiable health information for research purposes does not replace the informed consent to participate in a research study required by the Common Rule, the FDA Protection of Human Subjects Regulations, NCGS 122C-57 (f), 10A NCAC 26C.0200, 10A NCAC 26D.1300, or 10A NCAC 28A.0305.*

3.6.4 Alteration or Waiver of Client Authorization to Use or Disclose Individually Identifying Health Information for Research

A DHHS researcher may submit a request to an IRB or privacy board for a waiver or alteration of client authorization for the use or disclosure of individually identifying health information for research if the researcher determines that obtaining client authorizations is not feasible. For example, a researcher may need to request an alteration or waiver of requirement for client authorization for the use or disclosure of individually identifying health information for research in the following cases:

- The researcher cannot practicably obtain a potential research subject's authorization for the review of individually identifying health information in advance of contacting the potential subject; or
- The research will only involve the use of existing client records or specimens and no intervention, interaction, or direct contact of any kind with the research subjects will occur.

In the first case, an IRB or privacy board may elect to approve the researcher's request for a limited waiver of authorization that will permit specified access and use of individually identifying health information solely for prescreening and recruitment contact pursuant to the approved research protocol. In the second case, the volume and/or age of records to be examined during the research may be such that it would not be practicable for the researcher to obtain client authorization beforehand. If the risk to the client's privacy is minimal, the IRB or privacy board may also elect to approve a waiver in this instance.

DHHS researchers shall submit all requests for the alteration or waiver of client authorizations for research in writing to an institutional review or privacy board.
If the IRB or Privacy Board approves the request for alteration or waiver of client authorization, the board shall document that the documentation of the alteration/waiver of authorization approval shall also include the following elements:

- A statement identifying the IRB or the privacy board and the date on which the alteration or waiver was approved;
- A brief description of the individually identifiable health information for which use, or access has been determined by the IRB or the privacy board to be necessary to the research;
- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited procedures; and
- A signature from the chair of the IRB or privacy board, or from another member of the board who has been designated by the chair.

If a DHHS IRB or privacy board does not approve a request to alter or waive the client authorization requirement for research, the board must inform the researcher of the decision in writing. Similarly, if the board requires a change to the request for the alteration or waiver of client authorization prior to approving the request, the required changes must be documented and sent to the researcher.

If a research project is taking place at multiple sites and/or requires the use and disclosure of individually identifying health information created or maintained by more than one Office or DHHS Division (collectively referred to as 'multisite projects'), more than one IRB may be involved in research study reviews, or researchers participating in the multisite project may elect to use a single IRB. The same situation is expected to occur with Privacy Boards. In some circumstances, Privacy Boards and IRBs will coexist. Regardless, a DHHS Division and Office may rely on a waiver or an alteration of authorization approved by any IRB or Privacy Board, without regard to the location of the approver. However, DHHS Divisions and Offices may elect to require duplicate IRB or Privacy Board reviews before disclosing individually identifying health information to requesting researchers.

- Researchers external to DHHS covered health care components that identify potential research subjects during their reviews preparatory to research must submit a written request to the DHHS Division and Office if they want the them to notify the client about a possible opportunity to participate in the research.

- Researchers internal to DHHS covered health care component's workforce may contact the client directly for the purposes of recruitment for the research study. However, DHHS researchers must obtain authorization from a client who has indicated interest in participating in a study prior to asking the client any screening questions that involve individually identifying health information.

Note: *If the preparatory research activity involves human subjects research (e.g., research subject recruitment, prescreening), the preparatory research activity must be reviewed and approved by an IRB and must satisfy the informed consent requirements unless otherwise waived by an IRB.*

3.6.5 De-Identified Health Information

The DHHS Divisions and Offices are unaware of a means by which the information could be used alone or in combination with other information to identify a client who is the subject of the information; **and** a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (e.g., Statistician I or II):

- Determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify a client who is the subject of the information; and
- Documents the methods and results of the analysis that justify such determination.

The following identifiers for the client or the relatives, guardians, employer, or household members of that client are removed:

- Names;
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geocodes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
    - The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people; and
    - The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Facsimile numbers;
- E-mail addresses;
- Social Security Numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code that can be re-identified without the use of the code key or knowledge of the method used to re-identify the information.

3.6.6 Use of Limited Data Sets in Research

DHHS Divisions and Offices may use or disclose a limited number of individual identifiers via a 'limited data set' for research without client authorization or IRB/Privacy Board alteration or waiver of authorization whenever the limited data set will meet the researcher's request.

To qualify as a limited data set, only the following identifiers for DHHS clients or relatives, guardians, employers, or household members of those clients can be associated with the health information:

- State, county, city or town, and/or ZIP Code;
- Birth date, admission date, discharge date, and/or date of death;
- Age; and/or
- Any unique identifying number, characteristic, or code, except for the following:
- Social Security Numbers;
- Medical record numbers;

- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers; and
- Device identifiers and serial numbers.

All other individual identifiers such as name, address, telephone number, etc. must be removed from the data before the resulting information can be considered a limited data set.

3.6.7 Research Requests Received from Organizations External to DHHS

All requests for access to health information (e.g., individually identifying health information, limited data sets, de-identified health information) for research purposes, including those from researchers external to DHHS, must be submitted in writing to DHHS Divisions and Offices via the Request for Access to Data form. In addition to the Request form, researchers must submit the following documentation, as indicated on the form for their type of request:

- IRB approval letter for the research protocol;
- Informed consent forms for research signed by DHHS clients that have agreed to participate in the research study as subjects, or IRB approval of informed consent alteration or waiver;
    - Either: Authorization forms signed by DHHS clients that have agreed to become research subjects;
    - IRB/Privacy Board approval of client authorization alteration or waiver; or
    - Request that the DHHS Division and Office obtain client authorization Upon DHHS Division and Office request, documentation of the decedent status of the clients who is the subject of the individually identifying health information requested.

    Note: *If the researcher does not specify clients, but requests individually identifiable health information for "deceased clients" in general, then the DHHS covered component will not need to request proof of client death.*

DHHS researchers may disclose individually identifying health information that has been gathered or created during the research study if the disclosure is:

- Permitted by client authorization;
- Permitted by the approved alteration or waiver of authorization;
- Permitted by the data use agreement;
- Made to the sponsor of the study if the protocol includes an FDA regulated product or activity for which the sponsor is responsible, and the disclosure is for the purposes of quality, safety, or effectiveness (e.g., adverse event/safety reports for investigational new products);
- Made to a health oversight agency that is performing oversight activities authorized by law (e.g., disclosure to the Office for Human Research Protections for the purposes of determining compliance with the Common Rule); or
- Required by law (e.g., disclosure to cancer registries, other public health reporting).

If a revision to the authorization or alteration/waiver of authorization is necessary to allow the desired disclosure, an IRB or Privacy Board must approve the revision to the protocol. If the terms of the data use agreement must be changed to permit the disclosure, a revised data use agreement must be signed by the researcher and the covered component.

Individually identifying health information gathered during the research study may not be included in presentations or publications of any type unless explicitly permitted by:

- The client via authorization or informed consent for research;
- Wavier of the client's authorization by an IRB or Privacy Board;
- Waiver of the client's informed consent by an IRB; or
- The data use agreement signed by the DHHS Division and Office disclosing the health information and the researcher.

DHHS Divisions and Offices may not allow the authorization, alteration/waiver of authorization, or data use agreement obtained for one research project to be used for another research project. However, the IRB or Privacy Board may reanalyze such disclosures and grant a waiver for other studies.

3.6.8 Retention of Research Documentation

DHHS Division and Offices receiving requests for access to individually identifying health information for research shall maintain a copy of the following in the client records:

- The approved request for access to health information for research. The research protocol and IRB letter of approval;
- Client authorization or IRB/Privacy Board documentation of approved alteration/waiver of authorization; and
- Client informed consent or IRB documentation of approved alteration/waiver of informed consent.

Research documentation filed in the client record must be retained according to the DHHS Division and Office's retention and disposition schedule for such records.

DHHS researchers must maintain copies of authorizations for research and approved waivers of authorization for a minimum of six (6) years from the date of creation, or the date on which the document was last in effect, whichever is later.
Accounting of Disclosures of Individually Identifying Health Information for Research Purposes
Clients have a right to request access to an accounting of all disclosures of their individually identifying health information for research purposes, unless such disclosure was made:

- Pursuant to the client's authorization; or
- As part of a limited data set.

Similarly, clients will not receive an accounting of disclosures of their health information if the information was de-identified. Documentation of disclosures must be kept in the circumstances listed below and provided to clients upon their request:

- Disclosures pursuant to an IRB or Privacy Board alteration or waiver of authorization;
- Disclosures used in preparation of a research protocol; or Disclosure of a decedent's individually identifying health information used for research.

3.7 Marketing and Fundraising

DHHS Divisions and Offices shall not disclose individually identifiable health information about clients without authorization for marketing or fundraising purposes. Such authorization must include the specific reason for using the client's information.

Guidelines

DHHS Divisions and Offices shall not disclose, sell, or coerce a client to permit disclosure of individually identifiable health information for marketing purposes without the authorization of the client who is the subject of the confidential information or the client's personal representative. This prohibition includes the disclosure, use, or selling of prescription drug patterns.

- **Exception**: DHHS Divisions and Offices must obtain an authorization for marketing except when the communication is in the form of:
    - Face-to-face communication made by an agency to a client or
    - Promotional gift of nominal value provided by DHHS.

  This provision allows the discussion of products or services as well as provide sample products without restriction.
  The health care services listed below are common communications that a client generally expects to receive as part of his/her continued health care services and are not considered marketing:
    - Disease management,
    - Wellness programs,
    - Prescription refill reminders, and
    - Appointment reminders.

3.7.1 Permitted Communications Not Considered Marketing

The health care services listed below are common communications that a client generally expects to receive as part of his/her continued health care services and are not considered marketing:

- Disease management,
- Wellness programs,
- Prescription refill reminders,
- Appointment reminders.

3.7.2 Fundraising Activities

DHHS Divisions and Offices performing fundraising activities, including appeals for money and sponsorship of events, may internally ***use*** only dates of treatment and demographic information, unless the client or the client's personal representative gives authorization for more expansive use of the client's individually identifiable health information. Demographic information that may be disclosed without authorization typically includes:

- Name,
- Address,
- Other contact information,
- Age,
- Gender,
- and Insurance status.

Guidance:

- Disease-related information such as diagnosis may not be used in fundraising. In addition, information about the component from which a client received services also cannot be used for fundraising purposes without the client's authorization if that information could reveal the nature of the diagnosis, service, or treatment the client received.

- DHHS Divisions and Offices that allow clients to participate in fund-raising activities (e.g., raffle to raise funds to help pay for an off-campus trip for a patient care unit) must ensure that the client's participation is voluntary. For incompetent clients, authorization from the client's guardian is required before the client can participate in such fund-raising activities.

- DHHS Divisions and Offices may ***disclose*** a client's dates of treatment and demographic information for fundraising purposes without the client's authorization only as follows:
    - To a covered health care component's business associate, pursuant to a business associate agreement;
    - To an agency-related foundation, unless prohibited by law;
    - The agency has included in their "Notice of Privacy Practices" that a client's individually identifiable health information may be used or disclosed for fundraising purposes;
    - When clients are sent fundraising materials that include a description of how the client may opt-out from receiving any further fundraising communications; and
    - Reasonable efforts have been made to ensure that clients who decide to opt-out from receiving future fundraising materials are not sent any materials from that point forward.

3.7.3 Authorizations

An authorization for the purposes of marketing and fundraising must state that the purpose of the disclosure is for marketing or fundraising activities and denote whether the individual's health information will be disclosed to a third party. Fundraising materials must describe how an individual may opt-out of receiving any further fundraising communications. Covered health care components must document a process for fulfilling those requests.

3.8 Alternative Confidential Communications

The Health Insurance Portability and Accountability Act (HIPAA) requires that a covered entity permit an individual to request alternative communication for PHI and PII. The covered entity must accommodate reasonable requests to receive the information requested by alternative means or at alternative locations.

Guidelines

Alternative confidential communication policy establishes requirements and guidance to all Department workforce members regarding protected health information (PHI), and personally identifiable information (PII). Alternative Confidential Communication shall mean communication from healthcare provider to patient or authorized patient representative by an alternative means or at

an alternative location. Examples of alternative communication include: alternative mailing address, alternative phone number, or using an alternative communication vehicle (email or phone) rather than the healthcare provider's standard method of communication.

Guidance:

- The following procedures define the process for complying with an individual's reasonable request(s) for alternative communication:
    - An individual request for alternative means of confidential communication must be made in writing utilizing the DHHS alternative confidential communication request form.
    - DHHS workforce must accommodate all reasonable requests to receive confidential communications by alternative means or at alternative locations and will not require an explanation from the individual as to the basis for the request.
    - Reasonable requests include using alternative telephone numbers, alternative addresses, refraining from leaving messages on answering machines, and refraining from mailing information to the individual. Unreasonable requests are those that would be too difficult technologically or from an administrative standpoint for the Department to accommodate.
    - The DHHS Division and Office Privacy Officials or designated staff will be responsible for receiving, processing, and responding to requests for alternative confidential communication.
        - If the request is for an alternative address, telephone, or e-mail, the designated staff member may approve it at the time of the request.
        - Approved requests for alternative communication must be communicated to all DHHS personnel who may be involved in the use or disclosure of the individual's PHI and PII. Each DHHS Division and Office Privacy Official will ensure appropriate internal alternative communication protocols are in place based on the DHHS Division and Office need.
        - If the request for alternative communication is denied, the reason for the denial must be documented on the alternative communication request form.
        - DHHS Division and Office Privacy Officials or designated staff member must contact the requestor in writing to inform of the reason for the denial.
        - The DHHS Division and Office Privacy Officials or designated staff member will document the acceptance or denial of an individual's request for alternative confidential communication request on the request form.
    - All alternative communication documentation relating to the request must be included in the patient's medical record.
    - To ensure compliance with alternative communication requests, DHHS workforce members must review the patient's medical record (paper or electronic) to determine whether a requestor has been approved for alternative confidential communication.

3.8.1 Denial Requests and Exceptions

- DHHS may deny a request for alternative confidential communication only if:
    - The request is unreasonable from a technological or administrative standpoint.
    - The requestor does not provide an alternative address or alternative method of contact.

3.9 Verification of External Requestors

In accordance with 45 CFR 164.514(H), Department workforce members will maintain confidentiality by obtaining identity verification of any external person or entity requesting the use and/or disclosure of PHI or PII either in person, verbally, or by written request. DHHS workforce members must verify the identity of any external person or entity through one of following verifications listed below.

Guidelines

DHHS will establish guidelines to verify an external entity's or an individual's authority to access protected health information (PHI) and personally identifiable information (PII).

3.9.1 Patient or Patient Representative Requestors

The following are approved methods for identity verification (any one of the following two options):

- Valid State/Federal Issued Photo ID (i.e., passport, government ID, state driver's license)
- Requestor must provide a minimum of three patient identifiers from the following list of acceptable identifiers below verbally or in writing as applicable:
    - Patient Social Security Number or last 4 digits of SSN (required)
    - Patient Date of Birth (required)
- Any one of the following:
    - Street Address
    - Medical Record Number
    - Birth Certificate

3.9.2 Third-Party Requestors

To verify if a requestor is truly a representative of the third party and that the request is on behalf of the third party, the following elements should be taken into consideration when reviewing the disclosure request:

- Letterhead: Request is on official company printed letterhead and PHI is to be mailed or faxed to the address or number printed on the letterhead and the address or number has been verified.
- Email Address: Request is received via e-mail from an e-mail address that identifies the third-party company (e.g., Jxxx.Dxx@Cigna.com) and the domain name has been verified. Ensure all PHI and PII disclosed via email is secured (DLP, ZixMail).
- Fax Coversheet with Company Logo: Requested information is mailed or faxed to mailing address or phone number contained in the coversheet.
- Photo ID: with official credentials when a third-party request is made in person (e.g., Law Enforcement and Public Officials).

3.9.3 Third-Party Requestors

Public officials or someone acting on the official's behalf should have a minimum of two of the following:

- Presentation of agency identification badge or credentials
- Proof of government status (e.g., photo ID issued by a government agency).
- A request written on the appropriate government letterhead.
- A written statement on the government letterhead written request that the person making the request is acting under the government's authority (e.g., a nonprofit company hired by a county health department to compile statistics on West Nile Virus).

3.9.4 Third-Party Requestors

- Disclosures from the facility directory
- Disclosures for disaster relief purposes
- Disclosures for the involvement in the patient care

3.10 Legal Occurrences

North Carolina law requires that certain individuals receive confidential information or records, upon demand; however, there may be federal laws that supersede the state requirements such as the federal Substance Abuse Regulations. HIPAA requires agencies to verify the identity and authority of individuals requesting individually identifying health information prior to releasing such information. Examples of individuals and groups who may need individually identifiable health information include:

- The chief medical examiner or a county medical examiner who is investigating the death of a DHHS client;
- The director of social services or designee who is investigating a case of known or suspected child abuse or neglect;
- The guardian ad litem representing a child in a case of known or suspected child abuse or neglect;
- A guardian ad litem representing a minor between the ages of 14 and 16 who wants to marry;
- The NC State Child Fatality Prevention Team/ the NC Child Fatality Task Force/ a community or local child protection and review team that are involved in the review of a child's death;
- The NC Secretary of DHHS when it has been determined that there is a "clear danger to public health;" and
- The state or local health director when pertaining to the diagnosis, treatment, or prevention of communicable disease.

NC law also requires that individually identifiable health information be released in the following circumstances:

- Known or suspected child abuse or neglect, child dependency, and child deaths believed to be due to maltreatment;
- Belief that a disabled adult is in need of protective services;
- Known or suspected cases or outbreaks of communicable diseases;
- Wounds and injuries caused by firearms;
- Illnesses caused by poisoning;
- Wounds or injuries caused by knives or other sharp instruments and a physician suspects a criminal act;
- Any other wound, injury, or illness wherein a treating physician suspects criminal violence was involved;
- Client-specific information for the central cancer registry; and
- Symptoms, diseases, conditions, trends in the utilization of health care services, or other health-related information that the State Health Director determines is needed to conduct a public health investigation of a possible terrorist incident.

Guidelines

DHHS Divisions and Offices may be required to use and/or disclose individually identifiable health information to an outside source for legal purposes. These situations shall be identified in this policy as "legal occurrences." This includes disclosing individually identifiable health information when responding to judicial and administrative proceedings, court orders (including protective orders), subpoenas, law enforcement, and other legal mandates.

3.10.1 Use and Disclosure Enforceable by Court of Law

Departments and Offices shall use or disclose individually identifiable health information as "required by law" wherein a federal, state, tribal, or local law compels an agency to make a use or disclosure of confidential information and that is enforceable in a court of law such as:

- Court orders;
- Court ordered warrants;
- Subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information;
- A civil or authorized investigative demand;
- Medicare conditions of participation with respect to health care providers participating in the program; and
- Statutes or regulations that require the production of information (including those that require such information if payment is sought under a government program providing public benefits).

All uses and disclosures of confidential information that are required by law must comply with and be limited to the requirements of the applicable law. Each DHHS Division and Office shall review other state and federal laws with which the agency must comply to determine if any provision of state law is contrary to a requirement of the HIPAA Privacy Rule. Such review is entitled "preemption analysis" and shall be conducted on a provision-by-provision basis of each state and federal law. If a state law relating to the privacy of individually identifiable health information is more stringent than a privacy regulation, state law shall not be preempted, thus providing greater privacy protections for a client.

3.10.2 Preemption

DHHS Divisions and Offices shall identify all of the state and federal laws and regulations that apply to that agency's components and shall review the requirements for using and disclosing individually identifiable health information. Agencies shall determine which law/regulation is more stringent and provides the most protections for the confidential information maintained on the agency's clients such as laws that:

- Prohibit or restrict a use or disclosure when the privacy regulation would permit it;
- Provide clients with greater rights of access or amendment to their health information;

- Require covered health care components to provide clients with more information about uses, disclosures, rights, and remedies;
- Require express legal permission from a client that is more limiting in scope or reduces the effect of the permission;
- Require covered health care components to retain or report information for the accounting of disclosures that is more detailed or is for a longer duration; or Provide greater privacy protection for the client.

Preemption analysis may be limited to those provisions in laws and regulations that apply to the use and disclosure of individually identifiable health information maintained by HIPAA covered health care components.

There may be instances where a client may be involved in a legal proceeding, either conducted by a court of law or a government agency. In such proceedings attorneys, judges and others involved with the proceeding may contact a DHHS agency to access a client's individually identifiable health information.

3.10.3 Authorization

As a rule, DHHS Divisions and Offices shall not disclose individually identifiable health information without first obtaining written authorization from the client who is the subject of the request or the client's personal representative, unless there is a court order that requires disclosure of confidential information. This rule applies when responding to:

- Requests presented by way of judicial or administrative proceedings;
- Subpoenas;
- Law enforcement officials (apart from when reporting a crime on the premises such as
- 'escapees' or 'missing children'); or
- Warrants.

Any administrative investigator or prosecutor, including investigators of Medicaid fraud that are not expressly authorized by federal or state law, must present a court order before an agency may disclose individually identifiable health information.

3.10.4 Authorization Not Required

There are various legal occurrences when DHHS Divisions and Offices may disclose individually identifiable health information without authorization. These instances include:

- Responding to court orders (including protective orders);
- Requests specifically authorized by state or federal law (as may be the case for certain health oversight activities, auditing, licensing, and disciplinary actions); or
- Responding to law enforcement officials when reporting a crime, so long as federal or state requirements do not forbid or limit the disclosure.

Guidance:	• **Subpoenas** When DHHS Divisions and Offices receive a subpoena for individually identifiable health information, it must be determined whether the subpoena resulted from a judicial or administrative order. If a court or administrative tribunal issues the subpoena, confidential information may be disclosed without authorization. A subpoena received from any other entity must be accompanied by an **authorization** from the client whose individually identifiable health information is being requested or a **court order** to release such information. • **Court Order** An order issued by a judge that specifically identifies the individually identifying health information to be disclosed. DHHS Divisions and Offices must comply with court orders. • **Involuntary Commitment** DHHS Divisions and Offices may disclose individually identifiable health information without authorization. Such disclosure is permitted by both state law and the HIPAA Privacy Rule when initiating the involuntary commitment process of an individual. • **Incompetency Hearing**

Disclosure of individually identifiable health information without authorization is permitted by both state law and the HIPAA Privacy Rule when initiating incompetency status.

- **Commitment Hearing and Rehearing**
  DHHS Divisions and Offices must provide certified copies of written results of examinations by physicians and records in cases of clients voluntarily admitted or involuntarily committed to the client's counsel, the attorney representing the state's interest, and the court in district or superior court hearings. Individually identifiable health information shall be preserved in all matters except those pertaining to the necessity for admission or for continued stay in a DHHS facility or commitment under review. The relevance of health information for which disclosure is sought shall be determined by the court with jurisdiction over the matter.

- **Forensic Clients – Court Ordered Exam**
  DHHS Divisions and Offices may send the results or the report of a client's mental examination to the clerk of court, to the district attorney or prosecuting officer, and to the attorney for the defendant when a mental examination has been ordered by the court.

- **Reporting Child Abuse or Neglect**
  DHHS Divisions and Offices are required to report child abuse and neglect. When reporting child abuse or neglect cases, demographic data and information relative to the suspected abuse or neglect may be reported without authorization to the DHHS Department of Social Services.

  Note: *The federal substance abuse regulations exception allowing programs to comply with mandatory child abuse reporting requirements under state law applies only to the initial reports of child abuse or neglect, and to a written confirmation of that initial report. All other reporting requires authorization from the client or the client's personal representative.*

- **Reporting Adult Abuse or Neglect**
  DHHS Divisions and Offices are required to report adult abuse and neglect, unless prohibited by federal law.
    - When reporting adult abuse or neglect cases, demographic data and information relative to the suspected abuse or neglect may be reported without authorization.

  Note: *The federal substance abuse regulations do not address adult abuse or neglect.*

- **Reporting Communicable Disease/Injuries/Danger**
  Divisions and Offices are required to report communicable diseases, serious wounds, and injuries. A responsible professional in the agency may disclose confidential information without authorization from the client when in the professional's opinion there is an imminent danger to the health or safety of a client or another individual; or when there is likelihood of the commission of a felony or violent misdemeanor.

- **Reporting for Master Client Index**
  Mental Health, and Developmental Disabilities, and Substance Abuse Services (MH/DD/SAS) facilities may furnish client identifying information to DHHS for the purpose of maintaining an index of client's service in state MH/DD/SAS facilities.

- **Legal Disclosures**
  DHHS Divisions and Offices may receive requests for individually identifiable health information that are legally allowed in specific situations, which are listed below.
- **Specialized Government Functions (i.e., Law Enforcement/Secret Service/FBI)**
  DHHS Divisions and Offices may disclose confidential information to agents representing specialized government functions as long as the request is reasonable, the identity of the requestor is verified, and there are no laws that prohibit such disclosure. Provide only the

following protected health information when assisting law enforcement officials for the purposes of identification and location:

- Name and address;
- Date and place of birth;
- Social Security Number;
- ABO blood type and Rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death (as applicable); and
- A description of distinguishing physical characteristics (e.g., height, weight, gender, race, hair and eye color, presence or absence of beard or mustache, scars, and tattoos)

- **Next of Kin**
  MH/DD/SAS residential facilities may disclose the fact of admission or discharge of a client to the client's next of kin whenever the responsible professional determines that the disclosure is in the best interest of the client; however, if the client is present or available and capable, the agency may not make such disclosure unless the client agrees, is provided an opportunity to object but expresses no objection, or the agency reasonably infers from the circumstances that the client does not object.

- **Internal Client Advocates (MH/DD/SAS)**
  An internal client advocate shall be granted, without authorization of a client or the client's personal representative, access to routine reports and other confidential information needed to fulfill the advocate's monitoring and advocacy functions. In this role, the advocate may redisclose such information to the facility director or other staff who are involved in the treatment of the client.

- **External Client Advocates (MH/DD/SAS)/Long Term Care Ombudsmen**
  External client advocates and Long-Term Care Ombudsmen must obtain prior written authorization from a client or the client's personal representative before being granted access to that client's confidential information, unless other federal laws permit access. Access to information shall be limited to that which is specified in the authorization.

3.10.5 Accounting of Disclosures

DHHS Divisions and Offices are required to keep a record of any paper, electronic, or verbal disclosure of individually identifiable health information made in response to the legal occurrences as specified in this policy.

Ch. 4 Client Rights Policies

4.1 Notice of Privacy Practices

Individuals served by a DHHS HIPAA-covered agency must be informed of their privacy rights and the agency's responsibility to protect their protected health information. The Department, as a covered entity, is required to provide a Notice of Privacy Practices in accordance with the HIPAA Privacy Rule, 45 CFR Subtitle A, Subchapter C, Part 164 and the HIPAA Omnibus Final Rule.

Guidelines

DHHS shall develop a general departmental Notice of Privacy Practices. This general Notice shall be designed to inform individuals of the department's legal duties and privacy practices with respect to the protected health information (PHI) it collects from them in general. Given that the scope of DHHS HIPAA-covered entities' use and disclosure may vary significantly, agencies designated as covered health care providers, health plans, or health care clearinghouses shall be required to develop and provide their own

individualized Notice of Privacy Practices. DHHS HIPAA-covered entities designated as internal business associates (IBA), however, will be allowed to use the general Notice of Privacy Practices, unless the DHHS Privacy Officer deems otherwise.

Both types of Notice of Privacy Practices shall outline the uses and disclosures of PHI the department/agency may make and shall notify individuals of their rights and the department's/agency's legal duties with respect to protecting their PHI. DHHS HIPAA covered entities shall only use and disclose PHI in a manner consistent with their Notice of Privacy Practices.

Upon request, an agency shall make its Notice of Privacy Practices available to any individual(s), whether the individual is an agency client. The agency shall provide such Notice in a manner consistent with all requirements specified within this policy.

Note: *DHHS HIPAA-covered entities that operate an Employee Health Service (i.e., provides treatment services to employees above and beyond testing services required as a condition for employment (e.g., TB Tine Test)) are required to provide employees with an Employee Health Service Notice of Privacy Practices.*

4.1.1 General Notice Requirements

Guidance:

- **Development of Notices**
  All Notice of Privacy Practices must contain the requirements outlined in 45 CFR § 164.520. In order to assist in ensuring that agencies' customized Notices contain all of the required elements, agencies should rely on the Notice of Privacy Practices Checklist and applicable templates for guidance.
  - Notices of Privacy Practices developed by DHHS HIPAA-covered entities shall be written in plain and simple language that a client, employee, or personal representative can easily read and understand.
  - Notices shall be made available in languages understood by a substantial number of clients served by each agency. At a minimum, each agency shall ensure its Notice is available in English and Spanish. DHHS Divisions and Offices can request Braille Notices from the Division of Services for the Blind for clients who request such a format. Notices shall contain the elements described in the Notice of Privacy Practices Required Elements section of this policy.

- **Notice Revisions**
  DHHS Divisions and Offices shall promptly revise their privacy Notice whenever there is a material change to their client's rights or the agency's uses, disclosures, legal duties, or other privacy practices described in the Notice. A revised Notice shall be available upon request on or after the effective date of the revision.
  - Except when required by law, an agency shall not implement a material change to any term of the Notice prior to the effective date of the Notice in which such change is reflected.
  - Prior versions of an agency's Notice shall be retained for a period of at least six (6) years from the date of the last Notice delivery or retained according to the agency's retention and disposition schedule, whichever is more stringent.

- **Provision of the Notice**
  DHHS HIPAA-covered entities shall provide a written copy of their Notice of Privacy Practices to any individual requesting a copy, regardless of whether the individual is an agency client.

  DHHS Divisions and Offices that operate an Employee Health Service shall provide a written copy of their Notice of Privacy Practices to each employee at their first treatment encounter.

  When providing individuals a Notice of Privacy Practices as required in this policy, an agency may provide their Notice to an individual by electronic mail (hereafter referred to as "e-mail") with a return receipt requested, if the individual agrees to an electronic Notice and such

agreement has not been withdrawn. If the agency knows that the email transmission failed, a paper copy of the Notice shall be provided to the individual. When a Notice is provided electronically, it shall meet the applicable delivery time requirements specified in this policy.

Any agency that maintains a Web site that provides information to the public about the agency's services or benefits shall prominently post its Notice on the Web site and make the Notice available electronically from the Web site. The Notice on the Web site shall reflect the most recent version.

DHHS HIPAA-covered entities do not have to provide their Notice to "inmates". "Inmates" include inmates from the NC Department of Correction and clients committed through the criminal justice system to a psychiatric hospital (i.e., clients sent for pre-trial evaluation; clients found not guilty by reason of insanity; clients found incapable to proceed to trial [House Bill 95]).

- **Approval Process**
  All Notices and revisions to Notices must be submitted to the DHHS Privacy Officer for final approval prior to public distribution. The DHHS Privacy Officer will obtain Attorney General Office approval for agency Notices and revisions to Notices when necessary. Also, the DHHS Privacy Officer is responsible for forwarding Employee Health Service Notices to the Division of Human Resources for approval.

4.1.2 Notice of Privacy Practices Required Elements

This statement shall be at the top of the Notice in a box: **"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."**

- The Notice shall contain a description of the types of uses and disclosures that the HIPAA-covered agency is permitted to make for treatment, payment, and health care operations. At least one (1) pertinent agency example shall also be included.
- A description of all other purposes for which the agency is permitted or required to use or disclose protected health information without the individual's written authorization.
- If a use or disclosure for any purpose is prohibited or significantly limited by another applicable law, the description of such use or disclosure shall reflect the more stringent law.

- For each purpose described, the description shall include sufficient detail to inform the individual of the uses and disclosures that are permitted or required by federal regulations as well as state and federal law.
- A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such an authorization.
- A statement that the covered entity is not permitted to use genetic information for underwriting purposes.
- A statement regarding the covered entity's obligations to maintain the privacy of an individual's PHI and of the individual's right to receive notification, in the event of a breach involving their PHI.
- In the event that the agency is a provider, the individual has the right to restrict disclosure of their PHI to a health plan, if the individual paid the provider, in full, for services rendered.
- If the agency intends to engage in any of the following activities, the activity description shall include a separate statement accordingly:
  - The agency may contact the individual to provide appointment reminders or information about treatment alternatives or other heath related benefits and services that may be of interest to the individual; or
  - The agency may contact the individual to raise funds for the agency. An individual has the right to opt out of receiving such communications.
- The Notice shall contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:
  - The right to request restrictions on certain uses and disclosures of protected health information, including a statement that the agency is not required to agree to a requested restriction;
  - The right to receive communications of protected health information confidentially, as applicable;

    - The right to inspect and copy protected health information;
    - The right to request amendment to protected health information;
    - The right to receive an accounting of applicable disclosures of protected health information; and
- The right of an individual, including an individual who has agreed to receive the Notice electronically, to obtain a paper copy of the Notice from the agency upon request.
- The Notice shall contain the agency's duties, as follows:
    - A statement that the agency is required by law to maintain the privacy of protected health information and to provide individuals with Notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;
    - A statement that the agency is required to abide by the terms of the Notice currently in effect; and
    - A statement that the agency reserves the right to change the terms of its Notice and to make the new Notice provisions effective for all protected health information that it maintains prior to issuing a revised Notice. The statement shall also describe how it will provide individuals with a revised Notice.
- The Notice shall contain a statement that individuals may complain to the agency and to the Secretary of the United States Department of Health and Human Services if they believe their privacy rights have been violated. A brief description of how the individual may file a complaint with the agency and a statement that the individual will not be retaliated against for filing a complaint shall also be included in the Notice.
- The Notice shall contain the name or title, and telephone number of a person or office to contact for further information.
- The Notice shall contain the date on which the Notice is first in effect, which shall not be earlier than the date on which the Notice is printed or published.
- Certain uses and disclosures of PHI will require an authorization, such as psychotherapy notes, disclosure of PHI for marketing and disclosures that constitute a sale of PHI.
- The Notice may also contain the following optional elements:
    - If an agency elects to limit the uses or disclosures that it is permitted to make, the agency may describe these limitations in its Notice, provided that the agency may not include in its Notice a limitation affecting its right to make a use or disclosure that is:
        - Required by law, or
        - If the agency, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person(s).

4.1.3 Additional Privacy Notice Requirements (Health Care Plan)

Guidance:

- **Provision of the Notice**
  A DHHS HIPAA-covered Division and Office designated as a health plan (i.e., Division of Medical Assistance) shall provide its Notice of Privacy Practices on a timely basis to its named insured (hereafter referred to as the "recipient"). New health plan enrollees shall receive a Notice no later than the time of enrollment. New enrollee Notices may be distributed at the time an application is filed, prior to determination of eligibility.

- **Notice Revisions**
  Whenever a DHHS health plan Notice is *materially* revised from the previous Notice, the revised Notice must be provided to the recipients then covered by the health plan within **60** days of the revision. When a Notice contains translated language other than English, changes in the Notice to correct or improve the translation **is not** considered a material change.

- **Other Notification**
  At least once every **three (3) years**, the health plan shall notify the recipients then covered by the plan of the availability of the Notice and how to obtain a copy. At a minimum, this notification shall be presented in both English and Spanish. This notification may be combined with other communications sent routinely to recipients (e.g., Medicaid cards).

4.1.4 Additional Privacy Notice Requirements (Health Care Providers That Have Direct Treatment Relationship with Clients)

Guidance:

- **Posting of the Notice**
  DHHS Divisions and Offices that are health care providers who have a direct treatment relationship (e.g., face to face) with their clients, and who have a physical site where health care is provided directly to individuals, shall post the Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the agency will be able to read the Notice. DHHS Divisions and Offices that operate an Employee Health Service shall post their Notice in the area where employees come for treatment.

- **Provision of the Notice**
  Except in an emergency, these agencies shall provide the Notice to clients or their personal representatives no later than the date of the first treatment service delivery, including service delivered electronically or via telephone. In an emergency treatment situation, the Notice shall be provided as soon as reasonably practicable.

  If a covered health care provider's first treatment of an individual is delivered electronically, the agency shall automatically forward an electronic Notice to the individual. The individual who receives the electronic Notice retains the right to receive a paper copy upon request. If the first treatment encounter with the individual is by telephone, the Notice must be mailed within one working day of the telephone encounter. Scheduling an appointment is not considered a treatment encounter.

  DHHS covered health care providers that provide residential services shall ensure that all clients are provided a Notice. Provision of the Notice can be met by having the client or personal representative read and return the Notice; however, the agency must provide the client or personal representative with a copy of the Notice upon request.

  DHHS covered health care providers that are required to comply with federal regulation 42 CFR Part 2, relative to substance abuse, must provide their Notice of Privacy Practices to their substance abuse clients at the time of <u>each</u> admission. Otherwise, DHHS covered health care providers that have a direct treatment relationship with their clients need to provide the Notice initially and when revisions are made as noted below in the *Revision of Notice* section.

- **Acknowledgement of Receipt of the Notice**
  DHHS covered health care providers with a direct treatment relationship shall make a good faith effort to obtain a written acknowledgment of receipt of the Notice from the client or personal representative, except in an emergency. If the first treatment encounter with the client is by telephone, mailing the Notice to the client and asking the client to return the signed acknowledgment in person or by mail shall be considered a good faith effort. When a Notice is delivered electronically, an electronic return receipt is considered a valid written acknowledgment of the Notice.

  Should a client or personal representative be unable to sign his/her name on the acknowledgment, an "x" or other mark/symbol is acceptable in place of a signature, as long as it is witnessed and documented, attesting to the validity of the signature.

  The Notice should provide a section for an acknowledgment. The DHHS Division and Office shall keep the signed page as documentation of the receipt of Notice.

The DHHS covered health care provider shall not refuse to treat a patient because he/she would not sign a written acknowledgment; instead, it should document the good faith effort to obtain the signature. Documentation of a good faith effort shall include the date the Notice and acknowledgment was given/mailed to the individual, how it was delivered (in person, mailed, etc.), and the reason the acknowledgment was not signed (such as, patient refused or did not mail acknowledgment back to the covered health care provider).

Each provider agency shall establish a tracking process to ensure that each client was asked to sign the acknowledgment and that the signed acknowledgment was retained, or a good faith effort documented.

The acknowledgment or good faith effort shall be filed in the client's medical record and retained in accordance with the agency's retention and disposition schedule for medical records, which shall be no less than six (6) years.

- **Revision of Notice:** Whenever a DHHS health care provider's Notice is *materially* revised from the previous Notice, the revised Notice shall be available to clients or personal representatives upon request on or after the effective date of the revision. If a written acknowledgment was previously obtained or a good faith effort documented, another written acknowledgment is not required when the Notice is revised. In addition, the revised Notice must be promptly posted in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider will be able to read the Notice. If the provider agency has a public Web site, the revised Notice shall be available on the Web site.

4.2 Rights of Clients

This policy ensures the Department is aware of the rights given to clients by the Health Insurance Portability and Accountability Act (HIPAA), and to provide direction to those DHHS Divisions and Offices for addressing such rights.

Guidelines

The Department shall establish and implement procedures that ensure the following rights of clients as delineated by the HIPAA privacy rule and other federal and state laws:

- Right to Confidential Communications
- Right to Adequate Notice of Use and Disclosure of Individually Identifiable Health Information
- Right to Obtain Paper Copy after Electronic Notice
- Right to Request Access/Inspect/Copies of Individually Identifiable Health Information
- Right to Request Amendment to Individually Identifiable Health Information
- Right to Accounting of Disclosures of Individually Identifiable Health Information
- Right to Request Privacy Restrictions for Individually Identifiable Health Information
- Right to a Contact Person to Whom Client May Lodge Privacy Complaint

The rights that are included in this policy apply to individuals served by DHHS health care providers and health plan recipients, unless otherwise specified. For simplification purposes, this policy shall refer to all such individuals as `clients', unless there is a difference in policy requirements.

The personal representative of a client who is acting on behalf of that person is afforded the same rights as the client unless otherwise specified by state or federal law, in accordance with the DHHS Privacy Policies.

Documentation required by the HIPAA privacy rule throughout this policy shall be retained at least six (6) years from the date of its creation.

DHHS covered health care components and internal business associates shall negotiate the procedures for complying with this policy.

4.2.1 Right to Confidential Communications

Each DHHS covered health plan must permit plan recipients to request to receive communications regarding health information from the health plan by alternate means or at alternate locations when requested by a plan recipient. The health plan must accommodate such requests by plan recipients if the request is deemed reasonable. The health plan may require plan recipients to clearly state that the disclosure of all or part of their health information, using the current communication method or location, could endanger the plan recipient.

Client Rights

- Each client of a DHHS agency has a right to request confidential communications by requesting that the agency contact him/her at a different location or by a different means when the agency needs to communicate with the client.

Agency Responsibility

- Each DHHS covered health care provider must establish accommodations for their clients, whose privacy is not assured in their daily lives, to request alternative means of communication about their health information. Such accommodations may include an alternative location and/or method of contact such as mail, e-mail, fax, or telephone. Covered providers must develop procedures for making reasonable efforts to comply with such requests from their clients; however, providers may not require an explanation from their clients regarding the basis for such request.

4.2.2 Right to Adequate Notice of Use and Disclosure of Individually Identifiable Health Information

Clients of DHHS Divisions and Offices have a right to be informed about how the agency may use and/or disclose their health information, as well as their rights and the agency's legal duties with respect to protecting the privacy of health information in their possession.

Each DHHS covered health care component must make their *notice of privacy practices* available to their clients, which explains how the component may use and/or disclose their individually identifying health information. This *notice* also describes the rights of clients to take action and the component's legal duties, with regard to the use and/or disclosure of individually identifiable health information created and/or maintained by the agency. The following situations included in each agency's *notice* directly affect client rights.

In an emergency treatment situation, the client has a right for the *notice* to be provided as soon as practicable after the emergency;

- Clients must be assured that whenever there is a material change in the agency's privacy practices, the agency will promptly revise and post their notice of privacy practices. Such changes shall not be implemented prior to the effective date of the revised notice, except as required by law; and
- Health Plan recipients must be assured that whenever a material change has been made to the health plan's notice, the plan will provide a revised notice within 60 days of the revision.

Guidance:	• DHHS Divisions and Offices must establish procedures for ensuring clients' right to adequate notice of the agency's privacy practices. The required procedures listed below directly affect client rights:
	  o Establish procedures that ensure clients are provided the agency's notice;
	  o Establish procedures that ensure existing health plan recipients are provided the Plan's notice by April 14, 2003, and thereafter at the time of enrollment;
	  o Determine who is responsible for ensuring the notice given to clients is current, that revisions are made timely, that the notice is prominently displayed in the agency when required and that the notice is distributed according to the agency's requirements;
	  o Establish procedures for obtaining written acknowledgement from the client or the client's personal representative of receipt of the covered health care provider's notice, including the agency's good faith efforts if written acknowledgement is not obtained; and

- Establish procedures to follow-up in emergency circumstances wherein the notice was not provided to a client.

4.2.3 Right to Obtain Paper Copy after Electronic Notice

Each client of a DHHS Division and Office may be given the opportunity to receive the agency's *notice of privacy practices* electronically; however, the client further has the right to request that a paper *notice* also be provided.

Each DHHS Division and Office may offer to provide its *notice of privacy practices* to agency clients by e-mail, if the client agrees. Any client who receives the *notice* electronically retains the right to obtain a paper copy upon request.

Guidance:

- DHHS Divisions and Offices must develop procedures that address providing clients with a paper copy of the agency's *notice.* The procedures shall include the following:
  - Establish procedures to ensure clients are provided the agency's notice, including paper and electronic methods.
  - Enforce the clients' right to be provided a paper notice, upon request.
  - Establish a process for covered health care providers with a direct treatment relationship to clients to obtain written acknowledgement of receipt of the notice, including good faith efforts associated with electronic notice.

4.2.4 Right to Request Access to Individually Identifiable Health Information

Each client of a DHHS Division and Office has the right to request access to inspect and obtain a copy of his/her health information for as long as the information is maintained by the agency in a designated record set. If the agency does not maintain the health information that is the subject of the client's request for access, but knows where the requested information is maintained, the agency must inform the client where to direct his/her request for access. Each client's request for access to his/her personal health information must be in writing. DHHS Divisions and Offices may require the requester to:

- Complete agency form for request;
- Submit own written request; or
- Submit electronic request via e-mail.

The client's right to request access to records applies only to those records that have been identified as a `designated record set'. If the same information requested by the client or personal representative is contained in multiple designated record sets, the agency can limit access to a single designated record set.

Guidance:

- DHHS Divisions and Offices must determine the process for addressing a client's request to access, inspect, and copy his/her records. All requests from clients or their personal representative must be in writing and forwarded to the agency's privacy official, or other designee, who is responsible for ensuring the request is processed in a timely manner, not to exceed 30 days (with a one-time 30 day extension if the record cannot be accessed within the original 30 days). The Department is required to notify the requester in writing of any extension outlining the reasons for the delay.

  DHHS Divisions and Offices must grant access to individually identifiable health information in designated record sets unless it is determined there may be grounds for denial. When access is granted, agencies may provide a summary of the client's record in lieu of the entire record, if

that is agreeable with the client and the client agrees in advance to any fees imposed by the Department for producing the summary.

- **Note:** *DMH/DD/SAS General Statutes require that client access be determined by an attending physician. If there is not an attending physician, access must be determined by the agency director or his/her designee.*

- A licensed health care professional may deny access to information in certain circumstances:
  - If it is believed such access is reasonably likely to endanger the life or physical safety of the client or another person;
  - If the information refers to another person (other than a health care provider) and access may cause substantial harm to that person; or
  - If the access is requested by the client's personal representative and access could cause substantial harm to the client or to another person.

- If access to health information is denied in whole or in part, the licensed health care professional is required to comply with the requirements listed below:
  - Determine if access to any other requested information in the designated record set should be allowed;
  - Provide the client and the agency's privacy official with a written explanation as to the reason for the denial, that includes;
  - The basis for the denial;
  - If applicable, a statement of the client's review rights; and
  - A description of how the client may complain to the agency, including the name or title and telephone number of the person to contact.

- If a client requests review of the denial to access individually identifiable health information, the DHHS Division and Office must designate a different licensed health care professional who was not directly involved in the original denial, as a reviewing official to review, within a reasonable period of time, the decision to deny access. The agency must promptly provide written notice to the client of the determination made by the reviewing official. DHHS Divisions and Offices are required to respond to the request in accordance with the reviewing official's decision.

- DHHS Divisions and Offices may deny access to specific health information, as listed below, without providing a client an opportunity for review:
  - Psychotherapy notes;
  - Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;
  - Health information maintained by covered health care components that is subject to the Clinical Laboratory Improvements Amendments of 1988;
  - Information created or obtained in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided the client was previously informed of the suspension and consents to it;
  - Access to records that are subject to the Privacy Act, 5 U.S.C. 552a may be denied if the denial of access would meet the requirements of that Act; and
  - Individually identifiable health information that was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

- Each client who has been granted access to review his/her health information also has the right to request a copy of all or part of the health information to which access was granted.

- If a client requests a copy of his/her health information or agrees to receive a summary or explanation of such information, DHHS agencies may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:
    - Copying, including the cost of supplies for and labor of copying the information;
    - Preparation of an explanation or summary of the health information, if receipt of an explanation or summary is agreed to by the requester; and
    - Postage, when the individual has requested that the copy, summary, or explanation be mailed.

Note: *DMH/DD/SAS agencies are bound by 10 NCAC 18D.0121 when determining fees for copying health information.*

4.2.5 Right to Request Amendment to Individually Identifiable Health Information

Each client of a DHHS Division and Office has the right to request amendment of his/her health information that is contained in a designated record set, for as long as the information is maintained in the designated record set. Amendments may include changing or adding information.

Each client's request for amendment to his/her personal health information must be in writing and must include the reason for requesting amendment. DHHS Divisions and Offices may require the requester to submit the request as follows:

- Complete division and office form for amendment;
- Submit own written request; or
- Submit electronic request via e-mail if e-mail is available to the client.

DHHS Divisions and Offices must document the titles of the persons or the offices responsible for receiving and processing requests for amendments by clients. Such documentation must be retained for at least six (6) years from the date of creation.

DHHS Divisions and Offices must act on a client's request for amendment no later than 60 days after receipt of the request. If the agency grants the amendment in whole or in part, the following steps must be taken:

- Identify all documents in the designated record set(s) that need(s) to be amended
  Note: *If the amended information is contained in multiple designated record sets, the amendment must be documented in each record set*);
- Allow insertion of the amendment as an addendum to the contested portion of the designated record set; however, the original portion of the designated record set may not be deleted;
- Inform the requester that the amendment is accepted and obtain the client's identification of, and agreement to have the agency notify the relevant persons with which the amendment needs to be shared; and
- Make reasonable efforts to inform and provide the amendment within a reasonable time to those identified by the client and to any business associates who have copies of the health information being amended.

Guidance:

- DHHS Divisions and Offices may deny a request to amend a client's health information if it determines that the information:
    - Was not created by the agency (or that the originator of the information is no longer available to evaluate the request for amendment);
    - Is not part of a designated record set;
    - Is excluded from the information to which a client may request access; or Is accurate and complete.

- DHHS Divisions and Offices must provide a timely, written denial to a client that is written in plain language and contains the following elements:
    - The basis for the denial;

    - The client's right to submit a written statement disagreeing with the denial and how the client may file such a statement;
    - A statement that if the client does not submit a statement of disagreement, the client may request that the agency include the client's request for amendment and the denial with any future disclosures of the health information that is the subject of the amendment; and
    - Description of procedures to file a complaint. Such description must include the name or title and telephone number of the contact person or designated office.

- DHHS Divisions and Offices must permit a client to submit to the agency a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The agency may reasonably limit the length of a statement of disagreement.

- DHHS Divisions and Offices may prepare a written rebuttal to the client's statement of disagreement. Whenever such rebuttal is prepared, the agency must provide a copy to the client who submitted the statement of disagreement.

- DHHS Divisions and Offices must, as appropriate, identify the health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the following to the designated record set:
    - The client's request for amendment;
    - The agency's denial of the request;
    - The client's statement of disagreement with the request denial, if any; and
    - The agency's rebuttal to a client's statement of disagreement with a request denial.

- If a client has submitted a statement of disagreement, the agency must include the appended material in the designated record set in accordance with the record keeping section above, or at the discretion of the agency, an accurate summary of such information, with any subsequent disclosure of the health information to which the disagreement relates.

  If a client has not submitted a written statement of disagreement, the agency must include the client's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the health information only if the client has requested such action.

  When a subsequent disclosure described above is made using a standard transaction that does not permit the additional material to be included with the disclosure, the agency may separately transmit the required material to the recipient of the standard transaction.

- DHHS Divisions and Offices that are informed by other agencies/components of an amendment to a client's health information must also amend the health information in its own designated record sets.

- Documentation of requested amendments and the disposition of such requests shall be retained for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later. Documentation that is maintained in the client record shall be retained in accordance with the General Schedule for State Agency Records.

- DHHS Divisions and Offices must develop the following procedures to address when clients request amendments to their health information:
    - Designating the persons or offices responsible for receiving and processing requests for amendment by clients;
    - Identifying reviewing official(s);
    - Developing a request form, if applicable;

- Developing guidelines for establishing response time;
- Establishing criteria to be used in determining acceptance or non-acceptance of requested amendment;
- Defining methods for processing amendments of paper and electronic records;
- Establishing process for notifying requester of decision;
- Establishing process for making reasonable efforts to provide amendment to persons identified by the client and any other persons, including business associates, that the agency knows has been provided health information that is the subject of an amendment, within 60 days of the date of the amendment; and
- Establishing process so that the billing is reviewed to see if it should be amended or changed to reflect the new information when the amendment affects a service for which billing or charges have already been submitted.

4.2.6 Right to Accounting of Disclosures of Individually Identifiable Health Information

Each client of a DHHS Division and Office has a right to receive an accounting of disclosures of his/her health information made by the agency at any time during the previous six (6) years. Such requests may not include dates prior to April 14, 2003. This includes any disclosures made to or by any business associate of the agency. Disclosures made as follows do not have to be included on an accounting of disclosures:

- Disclosures to the client;
- Disclosures made based upon signed authorization of the client or personal representative; or
- Disclosures for purposes of treatment, payment or health care operations.

Disclosures made to health oversight agencies or law enforcement officials may be temporarily excluded from an accounting if the covered agency has been notified by the oversight agency or law enforcement official that providing an accounting could impede the progress of their activities.

DHHS Divisions and Offices shall require requests for accounting of disclosures to be in writing and forwarded to designated staff for action. DHHS Divisions and Offices are required to act on such requests within 60 days after receipt of the request, unless there is good reason to extend the time to reply by another 30 days. Any extension requires the agency to provide a written statement to the requester regarding the reason for the delay and the expected completion date. Only one (1) extension is permitted per request. The DHHS Privacy Policy, *Client Rights Policies, Accounting of Disclosures* provides all the requirements the Department must follow. For purposes of this policy, DHHS Divisions and Offices must be familiar with the following basic information for each disclosure that is required to be tracked and would therefore be available to a client upon request:

- Date of disclosure;
- Name of covered entity or individual who received the information (and their address, if known);
- Description of information disclosed; and
- Brief statement of the purpose or reason for the disclosure.

DHHS Division and Offices must provide clients or their personal representatives the first accounting of disclosures free of charge in any 12-month period. Agencies may impose a reasonable, cost based fee for each subsequent request for an accounting by the same individual within the same 12-month period, provided that the agency informs the client in advance of the fee and provides the client with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. (Refer to DHHS Privacy Manual Policy on Client Rights and Accounting of Disclosures.

Guidance:	• DHHS Divisions and Offices must develop the following procedures to ensure their clients' right to an accounting of disclosures of their health information. (Refer to the DHHS Privacy Policy Manual on Client Rights Policies, Accounting of Disclosures for detailed requirements for accounting of disclosures.):
	  o Designating the person(s) or office(s) responsible for receiving and processing requests for accounting of disclosures by clients;
	  o Identifying reviewing official(s);
	  o Developing request form, if applicable;
	  o Developing guidelines for establishing response time;
	  o Establishing criteria to be used in identifying accountings;
	  o Establishing process to ensure required disclosures are routinely documented;
	  o Establishing process for making reasonable efforts to provide accounting to clients within 60 days of request;
	  ▪ Determining any charges and establishing a basis for making such determinations; and
	  ▪ Maintaining audit trails that track client requests for accountings.

4.2.7 Right to Request Privacy Restrictions for Individually Identifiable Health Information

Each client of a DHHS Division and Office has the right to object to, and request restrictions on, how his/her health information is used or to whom the information is disclosed. Clients can make such requests/objections even if the restriction affects the clients' treatment or payment for that treatment or other health care operation activities. Use and disclosure of health information for treatment, payment, or other health care operations is oftentimes permitted by state and/or federal law without the client's authorization or consent. The client may want to limit the health information that is included in any of the following:

- DHHS Division or Office directories;
- Health information that is provided to family or friends who are involved in the client's care;
- Payment of medical bills; or
- Health information that is provided to authorities involved with disaster relief efforts.

DHHS Divisions and Offices are not required to agree to any requested restrictions. However, if a restriction is agreed to, it is binding and agencies may not use or disclose information in violation of the agreement, unless otherwise allowed or required under other DHHS policies. For example, an agency may disclose restricted information to permit emergency treatment. An agency is also not bound by restrictions when a disclosure is required by law. DHHS agencies are encouraged to require client request for restrictions to be in writing.

DHHS Divisions and Offices must establish procedures to address the following processes for ensuring clients' right to request privacy restrictions of their health information.

- Designating the person(s) or office(s) responsible for receiving and processing requests for privacy restriction;
- Determining the acceptable method(s) for requesting restriction(s);
  - Developing process for taking action on request; and
  - Establishing documentation requirements.

Guidance:	• DHHS Divisions and Offices must establish procedures to address the following processes for ensuring clients' right to request privacy restrictions of their health information.
	  ○ Designating the person(s) or office(s) responsible for receiving and processing requests for privacy restriction;
	  ○ Determining the acceptable method(s) for requesting restriction(s);
	  ▪ Developing process for taking action on request; and
	  ▪ Establishing documentation requirements.

4.2.8 Client Requests

Each DHHS Division and Office may determine whether to require such requests from clients to be in writing, or whether the agency will accept verbal requests. Verbal requests must be documented. The client must specify his/her preferred alternative means or location; and the agreement reached by the client and the agency must be documented.

4.2.9 Department Assurance and Procedures

Internal procedures must be developed so all workforce members who are engaging in communications with a client who has requested and received an agreement to use alternative means of communication are aware of the need to use other agreed upon channels in order to protect the client. An DHHS Division and Office could face serious liability if a client was harmed due to failure of staff to follow the agency's agreement to use alternative communications.

DHHS Divisions and Offices must develop procedures that address the following processes for processing confidential communication requests:

- Establishing how the requests will be submitted (orally or writing). Identifying who in the agency is responsible for reviewing the request to decide if it will be accepted;
- Establishing the process to notify the client of the agency's response to the request;
- Establishing the process to document the alternate means of communication;
- Identifying methods to be used to communicate changes to affected staff; and
- Ensuring future communications are consistent with the agreement.

4.2.10 Agreement or Denial of a Request for Restriction

Guidance:	• DHHS Divisions and Offices must establish procedures for processing clients' requests for restricting the use and/or disclosure of their health information, including the agency's process when request is agreed to and when request is denied. Procedures must ensure client's request is processed within 60 days of the request and client is fully informed of the decision.
	
	• If the restriction is agreed to, the following procedure must be implemented:
	  ○ The agency must honor the restriction;
	  ○ The restriction must be communicated to the agency staff in an approved manner; and;
	  ○ Documentation of the approved request must be provided to the client.
	
	• If the request for restriction is denied, the following procedure must be implemented:
	  ○ The agency's denial of the request shall be documented according to agency requirements; and
	  ○ Documentation of the denied request must be provided to the client.
	
	• DHHS Divisions and Offices may terminate an agreement to a restriction at any time. If the client agrees to the termination by the agency, previously restricted information may be used

or disclosed as if a restriction never existed. If a client objects to the termination, the termination is still in effect, but only with respect to the health information created or received after the client is informed of the termination of the restriction.

- DHHS Divisions and Offices must develop procedures that address the following processes for terminating a client-requested privacy restriction.
    - Documentation of written or oral agreement must be maintained;
    - The agency must inform the client that it is terminating its agreement to a restriction and that such termination is only effective with respect to health information created or received after it has so informed the client;
    - Subsequently, the restriction shall be removed, and such action shall be documented; and
    - Any documentation that alerted staff to the restriction must be removed (e.g., any "flag" in records/forms, etc.).

- If a DHHS Division or Office has agreed to a restriction but the client who requested the restriction is in need of emergency treatment and the restricted health information is needed to provide the emergency treatment, the DHHS Division or Office may disclose the health information to a health care provider to provide such treatment.

- If such health information is disclosed in an emergency, the agency must inform the health care provider to whom the information was disclosed not to further use or disclose that health information.

- DHHS Divisions and Offices must address the following processes when allowing clients to request restrictions on the use and/or disclosure of their health information.
    - Designating the person or office responsible for receiving and processing requests for restricting use/disclosures by clients;
    - Developing restriction request form, if applicable;
    - Developing guidelines for establishing response time;
    - Establishing criteria to be used in approving/denying restrictions;
    - Establishing process to ensure all restrictions are documented timely;
    - Establishing procedures to inform agency staff of approved restrictions, as well as termination of restrictions; and
    - Identifying documentation requirements to support all the above decisions.

4.2.11 Client Right to File a Complaint

Guidance:

- Each client of a DHHS Division and Office has the right to submit a complaint if he/she believes that an DHHS Division or Offices has improperly used or disclosed his/her individually identifiable health information, or if a client has concerns about the privacy policies of DHHS or concerns about DHHS compliance with such policies.

- Each DHHS Division and Office is required to identify a person or office in the agency that clients may contact if they have questions or concerns about the DHHS Division and Office's privacy policies and procedures, or if clients would like to submit a complaint regarding the use and disclosure of their health information.

- DHHS Divisions and Offices must provide a process for clients to submit a complaint for any of the following reasons:
    - If they feel their privacy rights have been violated;
    - If they want to file complaints about the DHHS Division and Office privacy policies and procedures; and/or
    - If they want to file a complaint about the DHHS Division and Office's compliance with their privacy policies and procedures.

- Such process shall ensure no retaliation may be taken against a client for filing a complaint against the DHHS Division and Office.

- DHHS Divisions and Offices are also required to inform clients of a contact in the U.S. Department of Health and Human Services should they wish to submit a complaint to that level. Agencies are required to include this information in their Notice of Privacy Practices.

- DHHS Divisions and Offices must develop procedures that address the following processes when ensuring clients' right to submit complaints about the DHHS Division and Office's privacy policies and procedures or about the DHHS Division and Office's use and disclosure of their health information;
    - Designating the person(s) or offices(s) responsible for receiving and processing complaints submitted by clients;
    - Identifying DHHS Division and Office contact person;
    - Determining acceptable method(s) for receiving complaints;
    - Developing complaint form, if applicable;
    - Developing guidelines for establishing response time;
    - Establishing criteria to be used in reviewing complaints;
    - Establishing protocols for addressing complaints;
    - Identifying persons involved in disposition of complaint;
    - Establish procedures for resolving complaints; and
    - Identifying documentation requirements to support all decisions.

4.3 Personal Representatives

DHHS Divisions and Offices shall recognize personal representatives who are authorized by the courts or by state or federal law to act on behalf of clients regarding their individually identifying health information in a manner consistent with all requirements within this policy.

Guidelines

Clients are authorized to make health care decisions on their own behalf and do not require a personal representative if they are:

- Adults (individuals 18 years of age or older) who have not been adjudicated incompetent;
- Individuals under 18 years of age who are married, serve in the Armed Forces of the United States, or who have been declared emancipated by a court of competent jurisdiction;
- A personal representative is usually required to make health care decisions about adults adjudicated incompetent and persons under 18 years of age (unless they meet the exception noted above).

Personal representatives may include the following:

- Person ordered by the court;
- Parent(s), of juveniles under 18 years of age;
- Person, other than parent, acting in loco parentis (of minor);
- Guardian as defined in chapter 35A;
- Person with health care power of attorney. The health care power of attorney document should define the scope of the personal representation with respect to access to individually identifying health information. The individual may also be referred to "health care agent" or "health care attorney-in-fact"; or
- Executor/administrator of estate (of deceased person).

Disclosures of individually identifying health information to a personal representative is required (with the exception of those situations described in this policy) only if disclosure to the client is required.

Guidance:

- Each DHHS Division and Office shall develop and implement procedures for determining who qualifies as a personal representative. These procedures shall include the identification of persons in the DHHS Division and Office who are responsible for confirming the legal status of each individual identified as a personal representative of a client.

- The personal representative's name, address and relationship to the client shall be documented in the client's record so that all staff are aware of who is authorized to approve or deny the use and/or disclosure of the client's individually identifying health information. Documentation should also include the name of the staff member confirming the legal status of the personal representative and the date that such legal status of the personal representative was determined.

- Procedures shall be developed and implemented that outline steps to be taken should the DHHS Division and Office be unable to recognize an individual as a personal representative.

4.3.1 Unemancipated Minors

Generally, a parent, guardian, or other person acting in loco parentis who has the authority to make health-related decisions on behalf of a client who is an unemancipated minor must be treated as a personal representative and may access and control health information about the minor.

Guidance:

- The minor may control his/her health information related to a particular service and exercise the privacy rights afforded to the client in any of the following circumstances:
    - If the parent, guardian or other person acting in loco parentis has agreed to a confidential relationship between the minor and the physician for a health care service;
    - Where a minor can obtain a particular health care service under their own consent (for example, as specified in NCGS 90-21.5), and no other consent is required by law (regardless of whether such consent has actually been obtained), the parent, guardian or other person acting in loco parentis may not be treated as the personal representative, unless the minor requests they be treated as such;

- If the minor may lawfully obtain care without consent of a parent, guardian or person acting in loco parentis, and the minor, a court, or another person authorized by law consents to the service (for example, as specified in NCGS 90-21.7), the parent, guardian or person acting in loco parentis may not be treated as the personal representative; or
- In DHHS Divisions and Offices under the Division of Mental Health, Developmental Disabilities and Substance Abuse Services, both the minor and parent, guardian or person acting in loco parentis must authorize disclosure of the minor's health information when either of the following applies:
  - In DHHS Divisions and Offices designated as `substance abuse programs under 42 CFR Part 2,
  - when the minor's parent or guardian has consented to the minor's treatment for substance abuse; or
  - When disclosures are made to external client advocates.

- In the case of joint parental custody, either parent may be treated as the personal representative of the minor unless a court order dictates otherwise.

- Disclosure of health information about a minor to a parent, guardian or person acting in loco parentis to avert a serious and imminent threat to the health or safety of the minor is permitted even if the minor obtained the health service without the consent of the parent, guardian, or person acting in loco parentis.

- Any individual who has legal authority to act on behalf of an adult or to act on behalf of an emancipated minor who has been determined to lack the capacity to make health-related decisions, shall be treated as a personal representative as it relates to the client's health information relevant to the matters on which the personal representative is authorized to represent the client.

- In the case of shared guardianship, both guardians must be treated as personal representatives and both have equal rights regarding decisions related to the client's individually identifying health information. Both guardians must signify agreement in order to execute a decision, unless a court order dictates otherwise.

4.3.2 Deceased Client

An executor, administrator, or other person who has authority to act on behalf of a deceased client or of the client's estate shall be recognized as the personal representative with respect to the deceased client's individually identifying health information. The next of kin of a deceased individual can be treated as the personal representative when there is no executor or administrator.
The following persons, in priority order, can be treated as the personal representative of a deceased individual with respect to authorizing anatomical gifts/organ donations and the individually identifying information pertaining to the making of the anatomical gift/organ donation:

- Spouse;
- Adult child;
- Either of the individual's parents;
- Adult sibling;
- Guardian of the person;
- Any other person authorized or under obligation to dispose of the body.

A DHHS Division or Office may disclose individually identifying health information to a funeral director as necessary to carry out their duties with respect to the decedent.

4.3.3 Exceptions

A DHHS Division or Office may decide not to treat an individual as a personal representative of the client if, in the exercise of professional judgment, the DHHS Division or Office determines that it is not in the best interest of the client to treat the individual as the client's personal representative, and that either of the following exists:

- The covered entity has a reasonable belief that the client has been or may be subjected to domestic violence, abuse, or neglect by such person; or
- That treating such person as the personal representative could endanger the client.

If the client is present for, or otherwise available prior to a disclosure, the DHHS Division and Office may disclose to a family member(s) or friend(s) individually identifying health information that is directly relevant to that person's involvement with the client's health care if the DHHS Division and Office meets one of the following criteria:

- Obtains the client's authorization to disclose to the parties involved in their care;
- Provides the client with the opportunity to object to the disclosure, and the client does not object (this provision does not apply to DHHS Divisions and Offices under the DHHS Division of Mental Health, Developmental Disabilities and Substance Abuse Services); or
- Reasonably infers from the circumstances, based on professional judgement that the client does not object to the disclosure.

If the client is not present for the disclosure, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the client's incapacity or an emergency circumstance, the DHHS Division and Office may use professional judgment to determine whether the disclosure is in the best interest of the client. If so, the DHHS Division and Office may disclose only the health information that is directly relevant to the family member/friend's involvement with the client's health care.

A DHHS Division and Office may use professional judgment and experience with common practice to make reasonable inferences of the client's best interest in allowing a person to act on behalf of the client to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of individually identifying health information.

A DHHS Division and Office may disclose the necessary individually identifying health information to notify or assist in the notification of family members, personal representatives, or other persons responsible for a client's care with respect to a client's location, condition, or death.

4.4 Designated Record Sets

A Designated Record Set is a description of health and/or business information that can be maintained in one or many areas within an DHHS Division or Office. The term *record* means any item, collection, or grouping of information that includes information (including individually identifiable health information) and is maintained, collected, used, or disseminated by or for a health plan or health care provider.

Designated Record Sets are maintained by or for a health plan or health care provider and include:

- Medical records and billing records of individual clients, maintained by or for a covered health care provider;
- Employee health records that are maintained separately from personnel records;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Categories of records that are used, in whole or in part, to make decisions about clients.

Guidelines

DHHS Divisions and Offices shall identify categories of records maintained, collected, used, or disseminated by the agency that contain individually identifiable health information including medical records and billing records maintained by health care providers, specified records maintained by health plans and other records used in making decisions about clients. Such records shall be termed "Designated Record Sets" and shall be considered the only personal health information records to which clients have a right to request access, amendment, and copies.

A process must be developed to evaluate the documentation maintained by the Department to determine those groups of records that should be categorized as Designated Record Sets. The defined process should ensure that the following information is gathered about the evaluated records:

- Documentation type (e.g., medical record);
- Basic content (e.g., assessments, reports, examinations);
- Location of the documentation (e.g., Medical Record Department);
- Contact person (e.g., agency privacy official);
- Paper/electronic documentation (e.g., paper);
- Documentation contains individually identifiable information (e.g., yes);
- Documentation is used to make decisions about the client (e.g., yes)

The following steps must be takin as part of implementation of Designated Record Sets:

- Identifying categories of Designated Record Sets requires an assessment of all documentation to determine which records should be included or excluded before further consideration is given to the categories to be classified as Designated Record Sets;
- Documentation must be maintained that supports the agency's assessment of its records for determination of its Designated Record Sets. Documentation may be maintained electronically or on paper;
- Such information must be kept current and available for reference should a client request access to his/her health information, including comments that identify any information included in a Designated Record Set that the client would not have a right of access, amendment, or copies;
- Documentation requirements must be maintained for a period of at least six (6) years.

Business Associates

Records created and/or maintained by an External Business Associate for services rendered to a DHHS Division or Office must be considered when evaluating documentation for Designated Record Sets. It is the responsibility of each DHHS Division and Office to ensure that a Business Associate Agreement is in place when required.

- Health information specifically created and/or maintained by External Business Associates, when acting on behalf of a DHHS agency, is subject to the client rights provisions to request access to or amendment of such information in accordance with the Business Associate Agreement. Copies of information that are also maintained by a health care provider or health care plan should not be included in the Business Associate's Designated Record Set.
- Internal Business Associates who maintain individually identifiable health information are subject to the requirements of this policy in identifying Designated Record Sets. This is accomplished by joint agreement of the DHHS agency and its Internal Business Associate(s).

Guidance:

- Documentation requirements must be assessed in order to identify those records that meet the intent of this policy. Health information in all types of media (e.g., paper, oral, video, electronic, film, digital) must be considered. Minimally, the following categories of records should be considered Designated Record Sets:
  - **Medical Records**
    - Identify what constitutes the medical records in your agency (e.g., paper records stored in medical record folders maintained in the Health Information Management Department; active medical records utilized by health care staff prior to client discharge).
    - If the agency uses an electronic medical record for all or parts of the medical record, specify if the Designated Record Set is the automated system or a copy produced from the automated system.
    - Specify if copies of records from other health care providers will be included as part of the Medical Record Designated Record Set.

    Copies may be included as part of the Designated Record Set for access only; clients may be required to go to the source of the information to request amendments.

  - **Business Records**

    Specify if the Designated Record Set is an automated system or a hard copy report produced by an automated system for the following:
    - Eligibility information maintained by health plans;

        - Enrollment records maintained by health plans;
        - Claims records submitted to or received from health plans;
        - Remittance Advices and records of payments;
        - Patient Statements;
        - Claims adjudication records;
        - Case or medical management records maintained by health plans.

    - **Other Records**
      Other records used by health plans and health care providers to make decisions about individuals. For example, documentation such as raw test data and laboratory reports maintained by various programs in the agency are considered "working records" and should be evaluated as to the benefit to clients to request access and amendment. Reports developed from working records that are filed in the medical record should be evaluated with the medical record as a whole and not as separate documentation. Examples of working records may include:
        - Raw test data from psychological tests;
        - Audio tapes (e.g., dictation tapes, taped sessions with clients/family that would not be considered psychotherapy notes);
        - Psychotherapy note;
        - Videos/photographs of clients used for teaching purposes;
        - Telemedicine;
        - Coding worksheets;
        - Utilization review worksheets;
        - X-ray film;
        - Working notes summarized and dictated into the client record

- **Exclusions**
    - Health information that is not used to make decisions about individuals should not be included in a Designated Record Set. Such information may be found in many types of records that include significant information not relevant to the client, as well as information about other persons.

    - Some records (e.g., administrative records, oversight records) that are maintained by the agency require independent evaluation to determine whether they should be considered a Designated Record Set, such as:
        - Quality Improvement records;
        - Risk Management records (including Incident Reports);
        - Copies of reports/documentation/forms already designated;
        - Cancer Registry information;
        - Research documentation;
        - Education records governed by Family Educational Rights Privacy Act (FERPA)

    - DHHS Divisions and Offices are ***not required*** to allow clients access to Designated Record Sets if a licensed health care professional determines that access to such information would not be in the best interest of the client or another individual, and such determination is documented.

    - DHHS Divisions and Offices are ***not required*** to amend, at a client's request, any information in a record that the agency knows to be true and accurate.

4.5 Accounting of Disclosures

In accordance with the HIPAA Privacy Rule, 45 CFR 164.528, covered entities are required to make available to an individual upon request, an accounting of certain disclosures of the individual's protected health information made during the six years prior to the request. For purposes of this policy Disclosure shall mean the release, transfer, provision of access to, or otherwise divulging of individually identifiable health information outside of the agency holding the information, and shall include disclosures made in *written*, *oral*, or *electronic* form. The Department will provide accounting of such request except as otherwise specified within this policy.

Guidelines

The Department's covered health care components internal business associates shall develop procedures for responding to requests by clients or their personal representatives for an accounting of the disclosures made about the client, and for ensuring the accountings are provided in a timely manner. Business Associate Agreements with external business associates shall include the requirement for providing the covered health care component with a listing of disclosures made by external business associates, upon request of the component.

The Department's covered health care components and internal business associates shall designate a staff member who is responsible for receiving requests for accounting of disclosures. It is strongly recommended that this responsibility be limited to one (1) person in the DHHS Division and Office. DHHS Divisions and Offices are encouraged to designate a privacy official as the designated staff member. Each agency shall document the title of the staff member responsible for receiving and processing requests for an accounting. Documentation related to the designation of the staff member must be maintained for at least ten (10) years.

Due to the complexity of this policy and the involvement of numerous clinical, professional, clerical, and administrative staff, as well as business associates who must ensure disclosures are accounted for, each agency will need to develop a system for routinely monitoring compliance with this policy.

4.5.1 Disclosure Exclusions/Inclusions

Exclusions. The types of disclosures listed below **<u>do not</u>** have to be included in the Accounting of Disclosures:

- Disclosures necessary to carry out treatment, payment, and health care operations such as:
    - Disclosures to other health care providers (treatment);
    - Eligibility, billing, claims management, medical necessity, and utilization review (payment); and,
    - Provision of individually identifiable health information to the NC Office of the Attorney General when representing the interests of a covered component (health care operations).

    Note: *The definition of 'health care operations' is designed to identify those activities of a covered component that support the component's ability to provide treatment to individuals or to pay or be paid for such health care. Many disclosures that are required by law do not significantly further a covered entity's health care operations; rather, they further other important public purposes such as reporting child abuse, injuries due to violence, domestic violence or elder abuse, or responding to court orders.*
- Disclosures made directly to the client who is the subject of the individually identifying health information or to the client's personal representative;
- Disclosures that are incidental to a use or disclosure that is otherwise permitted or required when covered components and business associates have implemented reasonable and appropriate administrative, technical, and physical safeguards to limit incidental, and avoid prohibited, uses and disclosures;
- Disclosures made pursuant to an authorization signed by the client or personal representative;
- Disclosures made to the facility's directory, to persons involved in the client's care, or for other permissible notification purposes Disclosures made for national security or intelligence purposes;
- Disclosures made to correctional institutions or law enforcement officials with lawful custody of an inmate if the individually identifying health information is necessary for:
    - The provision of health care to such clients;
    - Health and safety of the inmate or other inmates, officers, or other employees at the correctional institution;
    - Health and safety of clients and officers or others responsible for the transportation of inmates;
    - The enforcement of law within the correctional institution; and
    - The administration and maintenance of the safety, security, and good order of the correctional institution.

Note: *Disclosures made to law enforcement officers who bring or pick up clients from the DHHS Division of Mental Health, Developmental Disabilities, and Substance Abuse Services (DMH/DD/SAS) facilities do not have to be included in the accounting.*

- Disclosures of de-identified data or individually identifying health information that is part of a limited data set in accordance with DHHS Privacy Policy;
- Disclosures that occurred prior to April 14, 2003.

Inclusions. Other than the exceptions noted above, all other disclosures of individually identifiable health information **must** be included in the accounting and may include any of the types of disclosures listed below.

- Public Health Authorities,
- Surveillance,
- Investigations,
- Interventions,
- Foreign governments collaborating with federal public health authorities,
- Reporting vital events such as births and deaths,
- Required reporting of diseases or injuries such as communicable diseases or registries such as cancer and immunization registries,
- Social Services,
- Child abuse, neglect, or exploitation,
- Disabled adult abuse or neglect.

4.5.2 Tracking Disclosures

Department covered health care components shall develop a process for documenting and tracking the accounting of disclosures. For those types of disclosures that must be tracked, such processes must include tracking disclosures made by the component and their internal and external business associates of individually identifying health information that are disclosed either orally, on paper, or electronically. Disclosures may be tracked manually or in electronic form ensuring accurate and complete accounting of disclosures. Such process could include computerized tracking systems that can sort by individual and/or date or manual logs with one (1) log per client maintained in the client's medical record or other file. Each component shall ensure that appropriate staff and business associates receive training on the tracking process.

- Each covered component shall determine if documentation of disclosures will be maintained in a centralized (e.g., all accountings maintained in a single database accessible to appropriate agency staff and business associates) or de-centralized fashion (e.g., each location that discloses information maintains an accounting for their location only). Such determination should be based upon complexity of the component and their internal and external business associates and the number of locations disclosing information that would have to be tracked.

- If documentation of accounting of disclosures is de-centralized, the designated staff member shall identify all possible locations where disclosures may be made and where such accountings should be maintained; and shall ascertain if information about the client whose accounting is requested has been disclosed by any of the possible locations. It is the responsibility of the designated staff person to collect de-centralized accountings which may remain as many separate documents or be compiled into a single document.

- When disclosures are made to a single source for multiple clients, it is not necessary to track each disclosure by making a notation in each medical record that has been accessed. The covered component need only document the following:
    - The identity (and address if known) of the person/agency to which access was provided;
    - A description of the records and individually identifiable health information to which the subject has access;
    - The purpose for the disclosure; and
    - When access was provided.

  It would be sufficient, for instance, for the covered component to maintain a separate notation of such disclosures, applicable to all records so accessed. Then, if an individual request an accounting, the covered entity need only determine whether the individual's records were among the universe of records to which the person/agency was granted access. All individuals whose records were accessed in this fashion would receive the same accounting for the disclosure. For example, retrospective review of medical records for all clients treated by a health care provider may be required to identify cases of new or previously unknown infectious agents. If a client requesting an accounting was treated by the health care provider

during the period covered by the retrospective review, then the retrospective review should be included as part of the client's accounting.

- If access to a universe of records is provided for a discrete period of time, the accounting can include the range of dates (e.g., access was provided from August 1 to August 3, 2003; or during the week of August 10, 2003). If the disclosure is routinely made within a set period from an event, the component is permitted to provide the date of the event and the normal interval (e.g., hospital discharges reported on 15th of the following month for all discharges during the month of June 2003).

- Key features of an accounting of disclosures tracking system should include:
    - Allowing data entry from anywhere in the component;
    - Securing the information;
    - Tracking usage and compliance throughout the component;
    - Providing full auditing and reporting functionality;
    - Ability to track all disclosures that must be accounted;
    - Ability to track and report based on reason for disclosure;
    - Providing for temporary suspension of accountings for disclosures to law enforcement officials or oversight agencies;
    - Simplicity in using and understanding the process;
    - Cost effective mechanisms; and
    - The ability to provide on-demand accounting of disclosure reporting to the client or personal representative.

4.5.3 Request for Accounting of Disclosures

A client or personal representative's request for an accounting of disclosures must be made in writing. Each DHHS Division and Office shall designate the person within the agency who will be responsible for receiving and processing all requests for an accounting. DHHS Divisions and Offices shall forward such requests to the designated person for action.

The Department's covered health care components shall develop and implement procedures for clients or their personal representatives to request an accounting of disclosures; and shall negotiate procedures with their internal and external business associates to coordinate requests for accountings disclosed by the separate agencies/work units.

4.5.4 Providing Accounting of Disclosures to Client or Personal Representative

Guidance:	• If a health oversight organization or law enforcement official requests this temporary suspension orally, the component shall perform the following:
	  ○ Document the statement, including the identity of the agency or official making the statement;
	  ○ Temporarily exclude from the accounting of disclosures those disclosures made to an oversight agency or law enforcement official based upon the oral information in the statement; and
	  ○ Limit the temporary exclusion to no more than 30 days from the date of the oral statement unless a written statement is submitted during that time specifying the duration.

Upon request, a client or personal representative shall be provided a written accounting of all disclosures of individually identifying health information made after April 14, 2003 by the covered health care component. Such accounting may include any period of time within the six years prior to the date on which the accounting is requested.

Covered health care components are required to act on a request for an accounting of disclosures within 60 days after receipt of the request. If the component cannot provide the accounting within 60 days, the component may extend the time to provide the accounting; however, only one 30-day extension is permitted per request. Any extension requires the component to provide a written statement to the requester regarding the reason for the delay and the expected completion date.

- **Fees.** DHHS Divisions and Offices shall provide the client or personal representative's first request for an accounting at no charge to the client or personal representative. DHHS Divisions and Offices may charge the client or personal representative a reasonable, cost-based fee for any subsequent accountings within 12 months from the time the first request is received, provided that the fee includes only the cost of:
    - Copying, including the cost of supplies for and labor of assembling and copying the information; and
    - Postage, when the client has requested that the copy be mailed.

  DHHS Divisions and Offices must inform the client or personal representative in advance of the fee and provide the client or personal representative with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. Adequate time shall be allowed for the client or personal representative to withdraw the request before incurring any costs.

  Exception: DMH/DD/SAS agencies are bound by 10A North Carolina Administrative Code (NCAC) 26B .0105 when determining fees for copying health information, including accountings of disclosure.

4.5.5 Providing Accounting of Disclosures to health oversight agencies or law enforcement

Disclosures made to health oversight agencies or law enforcement officials shall be temporarily excluded from an accounting if the covered component has been notified by the oversight agency or law enforcement official that providing a client or personal representative with an accounting of the disclosures made to them could impede the progress of their activities (e.g., fraud investigation or investigation of possible criminal activities when a client should not be aware of such scrutiny). Such request from a health oversight agency or law enforcement official should be in writing; however, an oral request may be accepted with stipulations, as noted below. Suspensions requested in writing shall remain in effect for the duration specified in the written request, unless the request for suspension is rescinded earlier by the health oversight agency or law enforcement official.

Guidance:

- If a health oversight organization or law enforcement official requests this temporary suspension orally, the component shall perform the following:
    - Document the statement, including the identity of the agency or official making the statement;
    - Temporarily exclude from the accounting of disclosures those disclosures made to an oversight agency or law enforcement official based upon the oral information in the statement; and
    - Limit the temporary exclusion to no more than 30 days from the date of the oral statement unless a written statement is submitted during that time specifying the duration.

4.5.6 Request of Accounting for DMH/DD/SAS facilities.

In the facilities operated by DMH/DD/SAS, the request for accounting and copy of the accounting provided to the client shall be maintained in the client's medical record. All other covered components shall determine the most appropriate location for maintaining the documentation.

4.5.7 Contents of the Accounting of Disclosures to Clients or Their Personal Representatives

Guidance:

- Each accounting of a disclosure shall contain the following elements:
  - The date of the disclosure;
  - The name of the entity or person who received the individually identifying health information and, if known, the address of such entity or person;
  - A brief description of the individually identifying health information disclosed; and
  - Either a brief statement of the purpose of or reason for the disclosure that reasonably informs the client or personal representative of the basis for the disclosure;
  - A copy of any written request for disclosure by US DHHS for compliance purposes; or
  - A copy of a written request for a disclosure by a person or entity authorized to receive individually identifying health information for uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required (refer to DHHS Privacy Policy, Use and Disclosure Policies, Use and Disclosures).

4.5.8 Multiple Disclosures

Guidance:

- If multiple disclosures are made to the same person or entity for a single purpose, either to the US DHHS for compliance purposes or for uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required (refer to DHHS Privacy Policy, Use and Disclosure Policies, Use and Disclosures), the accounting should include the following:
  - The elements listed in the 'Contents of the Accounting' shall be provided;
  - The frequency, periodicity, or number of disclosures made to the common person or entity during the requested accounting period; and
  - The date of the first and last disclosure made during the requested accounting period.

4.5.9 Research Disclosures

Disclosures for research purposes wherein authorization for use and disclosure of individually identifiable health information for research purposes has been waived or is not required must be included in the accounting of disclosures; however, disclosures for research purposes wherein authorization has been obtained for use and disclosure of such information do not have to be included in the accounting of disclosures.

Guidance:

- If disclosures are made for 50 or more clients for research purposes, the accounting must include:
  - The name of the research protocol activity;
  - A plainly written description of the research protocol or activity, including:
    - Purpose for the research, and
    - Criteria for selecting particular records to be disclosed for the research;
  - A brief description of the type of individually identifying health information that was disclosed;
  - The date or period of time during which the disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
  - The name, address, and telephone number of the entity that sponsored the research, including the name of a contact person;

- The name, address, and telephone number of the researcher to whom the information was disclosed; and
- An indication that the individually identifying health information of the client may or may not have been disclosed for the particular research protocol or activity.

If the component provides the modified content described above (in lieu of the standard content for an accounting), upon request by the client or personal representative, the component shall assist the client or personal representative in contacting the researcher if disclosures for research purposes were made by the component.

4.5.10 Business Associates Disclosures

Guidance:

- The Department covered health care components must develop procedures that address the following processes for ensuring their clients' right to an accounting of disclosures of their health information and need to be coordinated between covered health care components and internal and external business associates:
  - Designate the person(s) or office(s) responsible for receiving and processing requests for accounting of disclosures by clients or personal representatives;
  - Develop training materials that ensure staff can differentiate disclosures that must be accounted for, from disclosures that do not have to be accounted for;
  - Determine the acceptable method(s) for requesting and receiving an accounting;
  - Develop an accounting request form;
  - Identify all areas within the component and their business associates where disclosures that must be tracked would be made;
  - Establish process to ensure required disclosures and accidental disclosures are routinely documented;
  - Establish process for making reasonable efforts to provide accounting to clients or personal representatives within 60 days of request and process for one 30-day extension, if needed;
  - Establish process for temporary suspension of certain accountings;
  - Determine if agency will handle multiple disclosures or research disclosures differently from standard accountings;
  - Ensure established process for accountings is correctly reflected in component's Notice of Privacy Practices;
  - Determine any fees and a process for informing clients of the fee;
  - Maintain audit trails that track client or personal representative requests for accountings;
  - Develop process for monitoring compliance with policy;
  - Maintain required documentation.

4.5.11 Retention

Each component shall retain the following documentation for no less than ten (10) years from the date the accounting request was received:

- Client or personal representative's request for an accounting;
- Copy of the accounting provided to the client or personal representative; and
- Title of the person or office responsible for receiving and processing accounting requests.

5.1 Business Associates (Internal/External)

The Department ensures that all individuals or organizations that perform specific functions, activities, or services on behalf of the Department involving the sharing of individually identifiable health information are appropriately identified according to The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as a "**business associate"**; and to further ensure that **"agreements"** are developed to support such contractual relationships, as appropriate. ***This policy shall apply to the following DHHS Divisions and Offices:***

- ***HIPAA covered health care components and***
- ***Internal business associates***.

It should be noted that the Omnibus Final Rule has expanded the definition of a business associate to include:

- Any downstream subcontractor that creates, maintains, receives or transmits protected health information (PHI) on behalf of a business associate, even if they have an indirect relationship with the covered entity;
- Health information organizations, e-prescribing gateways, or other persons that provide data transmission services to a covered entity that require routine access to PHI; and
- Any person that offers a personal health record to individuals on behalf of a covered entity.

Internal Business Associates. The department has been determined to be a hybrid entity. Each DHHS Division and Office is required to identify components that are covered by this HIPAA requirement. Some components that perform functions, activities, or services that involve the sharing of individually identifiable health information for, or on behalf of, covered health care components, creates a business associate relationship within this department. Such persons or entities ***within*** DHHS are health care components that are referred to as **"internal business associates"**.

External Business Associates. Components in other NC state government departments/agencies or external contractors ***outside*** of the Department that perform functions, activities, or services for, or on behalf of, a DHHS covered health care component, and involve the use, creation, or disclosure of individually identifiable health information are referred to as **"external business associates"**.

Functions, activities, and services performed by business associates that involve the use, creation, or disclosure of individually identifiable health information may include:

- claims processing or administration;
- data analysis, processing or administration;
- utilization review;
- quality assurance;
- billing;
- benefit management;
- practice management; and
- re-pricing.

Guidelines

The Department covered health care components are required to identify their ***internal*** business associates by recognizing all of the other DHHS Division and Office (or portions thereof) within the department that perform specific functions, activities, or services for, or on behalf of, the covered component when such functions or activities involve the sharing of individually identifiable health information.

DHHS ***internal*** business associates must also identify their internal business associates by recognizing any other health care component(s) within DHHS that perform such functions, activities, or services for, or on behalf of, the internal business associate that involves the sharing of individually identifiable health information.

The Department covered health care components and internal business associates must identify their ***external*** business associates by recognizing other NC state government departments/agencies and external contractors (public and private) that perform specific functions, activities, or services for, or on behalf of, the covered component or the internal business associate when such functions, activities, or services involve the sharing of individually identifiable health information.

Business associates, as well as their subcontractors who have access to PHI, are now directly liable for failure to comply with the HIPAA Privacy and Security Rules. If they fail to do so, they can be assessed civil and criminal penalties.

Note: *Incidental access to individually identifiable health information while performing duties that do not typically involve the use or disclosure of such information generally does not constitute a business associate relationship.*

5.1.1 Business Associate Agreements

The Department covered health care components and internal business associates must initiate agreements with their external business associates in order to share individually identifiable health information while performing specific functions, activities, or services for, or on behalf of, the covered health care component or the internal business associate. It is the responsibility of covered health care components and internal business associates to execute agreements with external business associates that provide satisfactory assurance that the business associate will appropriately safeguard individually identifiable health information.

A Business Associate is responsible for entering into Business Associate Agreements with its subcontractors. In turn, a subcontractor is responsible for entering into Business Associate Agreements with any of its own subcontractors "down the chain" of information flow.

This revised Business Associate Agreement template, developed by the NC Office of the Attorney General, is required when contracts are initiated by DHHS staff. Such addenda must be attached to the department's standard contracting template as specified in the DHHS Purchasing and Contracts Manual.

External Contractors

Certain external contractors may be considered part of the HIPAA covered component's ***workforce***, and therefore will not require a business associate agreement if the following criteria apply:

- The workstation of the person under contract is on the covered health care component's premises and
- The person performs a substantial proportion of his/her activities at this location.

Any external contractor who is considered part of the covered health care component's workforce must comply with that component's privacy policies and procedures.

Exclusions

BAA are not required with contract agreements between agencies within DHHS since the DHHS Privacy Policy Manual applies to all DHHS agencies.

Disclosure of individually identifiable health information from one health care provider to another for treatment, consultation, or referral does not require a business associate agreement.

Note*: For MH/DD/SAS agencies, a business associate agreement would not be required, but those agencies would have to initiate either a "service provider agreement", according to NC General Statutes, or would have to secure client authorization to disclose health information to a health care provider outside the agency.*

A business associate agreement is also not required when individually identifiable health information is disclosed to a health plan for payment purposes.

Breach and Violations

The Department's covered health care components and internal business associates are required to take reasonable steps to correct any known material breach or violation of any business associate agreement. If such steps are unsuccessful, the agreement must be terminated, if feasible; and if not, the problem must be reported to the DHHS Privacy Officer who will determine if further actions are warranted, which could include reporting the problem and correction attempts to the United States Department of Health and Human Services.

Enforcement

Should a covered health care component or internal business associate become a business associate of an agency external to DHHS, the Standard DHHS BAA must be utilized. Under no circumstances should any changes be made to this agreement without the

express agreement of the Attorney General's office. If specific terms need to be addressed, they should be addressed in the contract, not the Business Associate Agreement.

5.1.2 Identifying Internal and External Business Associates

Each DHHS Division and Office that has at least one covered health care component or internal business associate must evaluate specific functions, activities, and services that are provided for, or on behalf of, that component/business associate to identify all internal and external business associates as follows:

- Within the same DHHS division/office;
- Within other divisions in DHHS;
- Within other departments/agencies in NC state government; and
- Outside state government (external contractors).

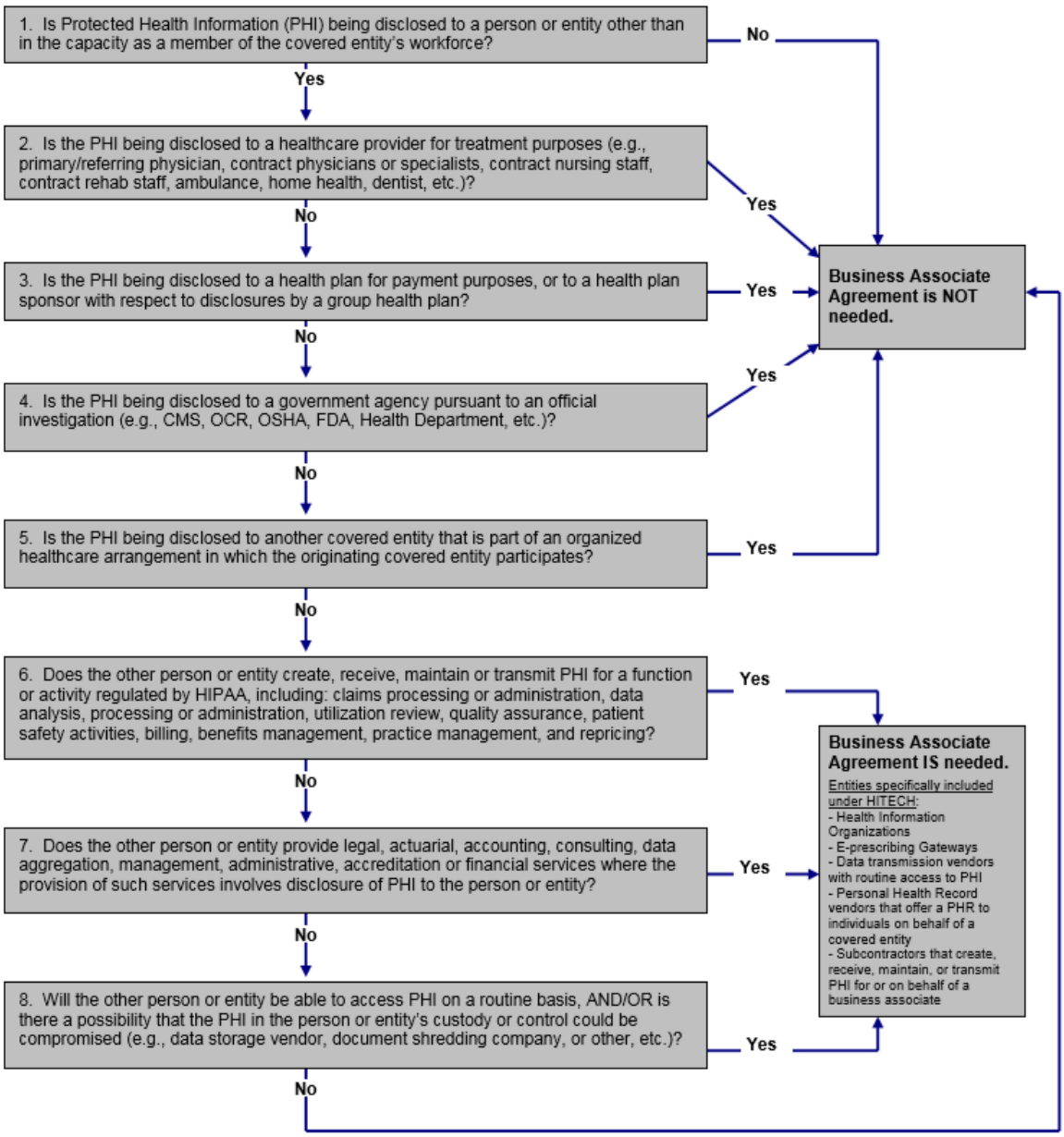
Guidance:

- Each agency must develop a process that identifies internal business associate relationships with other programs/units within the same division or with another division within DHHS. Components must maintain documentation of its internal business associates and update such information as internal business associates are added or deleted.

- Each agency must also develop a process that identifies external business associate relationships at the time the agency initially creates a contract with the external contractor. Renewal of a contract that has a Business Associate Addendum requires a review of the Business Associate Agreement as well, for renewal purposes.

- Covered components must identify all business associate relationships to standard contracts when entering contract information into the DHHS purchase and contracts database that monitors contracts. The Workgroup for Electronic Data Interchange (WEDI) has created a HIPAA/HITECH Business Associate Decision Tree to assist in making this determination.

HIPAA/HITECH
Business Associate Decision Tree



5.1.3 Contractual Documentation Requirements

There are no Business Associate Agreement contractual documentation requirements for services provided by internal business associates, other than the DHHS Division or Office general documentation requirements.

Guidance:

- Documentation of services provided by external contractors is accomplished through a DHHS standard contract. Documentation of business associate requirements is accomplished in an addendum to the contract. Business Associate agreements must be maintained for at least ten (10) years from the date of creation.
- Only contract templates created by the NC Attorney General's Office should be used for business associate agreements. These documents include all of the updated HIPAA requirements to which their contractors must agree before covered health care components are allowed to share individually identifiable health information.
- Beginning July 18, 2013, all new or amended DHHS contracts must be evaluated to determine whether a business associate relationship exists. If a business associate relationship does exist, a Business Associate Agreement must be in place. For HIPAA compliant BAAs executed prior to the publication of the Final Rule (1/25/13), the executed BAA may remain in effect until 9/22/2014, or such time as it needs to be revised, whichever comes first. If a new BAA needs to be created, it must be executed prior to September 23, 2013.

5.1.4 Termination of Business Associate Relationship

Should a DHHS Division or Department covered health care component or internal business associate become aware of a pattern of activity, or practice of an internal business associate that constitutes a material breach or violation of the internal business associate's obligation with respect to privacy of individually identifiable health information in its possession, such information shall be forwarded to the DHHS Privacy Officer for resolution.

Should a DHHS Division or Department covered health care component or internal business associate become aware of a pattern of activity or practice of an external business associate that constitutes a material breach or violation of the external business associate's obligations with respect to individually identifiable health information specified in a contract or other arrangement, reasonable steps should be taken to cure each breach, end the violation, and/or mitigate the consequences.

If such steps are unsuccessful, the covered health care component or internal business associate may, at its discretion:

- Terminate the contract or arrangement, if feasible; or
- If termination is not feasible, the DHHS Division or Office privacy official is responsible for reporting the breach to the DHHS Privacy Officer. The DHHS Privacy Officer is responsible for resolution, which may include reporting the problem to the US DHHS Secretary at:

Office for Civil Rights
U.S. Department of Health & Human Services Atlanta Federal Center, Suite 3B70
61 Forsyth Street, S.W.
Atlanta, Georgia 30303-8909
Phone: (404) 562-7886
Fax: (404) 562-7881

5.1.5 Tracking of Business Associates

Each DHHS Division and Office is required to track their internal business associates by maintaining current documentation of their internal business associates throughout the year. DHHS Divisions and Offices shall track their external business associates through the contracts that are entered into the department database for purchasing and contracts.

5.1.6 Training

Department covered health care components and internal business associates are not required to provide privacy training to their external business associates; nor are they required to monitor the privacy protections for individually identifiable health information that are instituted by their external business associates.

5.2 Acceptable Use of DHHS Information Systems

This policy defines the information system security responsibilities and acceptable use rights for employees, volunteers, guests, vendors and contractors (hereinafter, "**Users**") of North Carolina Department of Health and Human Services ("**DHHS**", or alternatively, the "**Department"**) resources.

Resources include all platforms (i.e. operating systems), all digital devices (e.g. computers, smart phones, tablets, mainframes, switches, routers, etc.), equipment (e.g. faxes, copiers, phones, etc.), network connections, applications (both developed in-house and acquired from third parties) and the data used, created by or contained within them.

Communications include but are not limited to: faxes, printed documents, recordings, phone calls, social media (e.g. Facebook, Google+, Twitter, Blogs YouTube, Instagram, etc.) and email.

See Figure 1 for the agreement "Workforce **User Certification of Notification and Agreement of Computer Use Policy".**

Guidance

Each DHHS Division and Office shall be responsible for ensuring that every individual seeking access to DHHS network and/or information systems reviews this policy and signs an acceptable use agreement based upon the terms specified in this policy. Users must sign the agreement form included herein before permission is granted to use the DHHS systems. DHHS Divisions and Offices may require additional agreements or policies regarding the confidentiality of specific types of information (e.g. medical records, client case files, personnel records, financial records, etc.). Such supplements may be more restrictive than this policy.

5.2.1 Roles and Responsibilities

All information and data resources to which users are given access are to be used only to conduct the activities authorized by the Department. The use of these resources must be conducted according to the policies, standards, and procedures instituted by the Department or on its behalf. All individuals with access to state-owned data are responsible for the protection and confidentiality of such data. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of Department, state, or federal laws which will result in disciplinary action consistent with the policies and procedures of the Department.

Users have a responsibility to ensure, to the best of their ability, that all public information disseminated via Departmental resources and communications is accurate. Users shall provide in association with such information the date at which it was current and a method by which the recipient can contact the staff responsible for making the information available in its current form.

Users are responsible for:

- Safeguarding the information entrusted to the Department from unauthorized use, disclosure, modification, damage or loss;
- Limiting the amount of information to the minimum required;
- Ensuring that the recipient(s) of the information is/are legally authorized to receive the information;
- Reporting weaknesses in computer security, misdirected information, breaches (suspected and confirmed) or incidents (including possible misuse or violation of this policy) immediately to the DHHS Division/Office Information Security Official (ISO), who will notify the DHHS Privacy and Security Office;
- Reporting theft, loss, or unauthorized disclosure of information.

5.2.2 Rights of Information Ownership

The Department and its DHHS Divisions and Office retain the rights of ownership to all resources and communications including but not limited to data, and related documentation developed by Users on behalf of the Department, regardless of location or resources used. All Department information resources remain the exclusive property of the State of North Carolina (NC) or the Department, unless otherwise prescribed by other contractual agreements.

5.2.3 Rules of Acceptable Use

The resources provided by the Department are to be utilized both responsibly and professionally; just because an action is technically possible does not mean that it is appropriate. Based on the following principles for acceptable use of Department resources, Users are:

- To protect the confidentiality, integrity and availability of departmental data by behaving in a manner consistent with DHHS's mission and complying with all applicable laws, regulations, policies, standards and guidelines;
- To comply with the policies, processes and guidelines for the specific resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence;
- To report any potential or identified privacy or security incident to the appropriate privacy or security staff;
- Allowed reasonable use (i.e. incidental personal use) of resources if:
    - Such use does not result in direct cost to the Department,
    - Such use does not cause embarrassment to the Department,
    - There is no negative impact on user's performance of their duties, and
    - The use is not prohibited (would not cause legal action against the Department);
- To respect the security and integrity of the department's resources;
- To be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to utilize resources and show restraint in the consumption of shared resources;
- To respect the rights and property of others, including but not limited to; privacy, confidentiality and intellectual property (e.g. copyright, trademarks, etc.);
- Bound by the department's respective contractual and license agreements when using third party resources;
- To cooperate appropriately during incident response and investigation of potential unauthorized or illegal use of resources.

5.2.4 Prohibited Uses

Users shall not:

- Connect personal devices or equipment to the network or applications that contain confidential data for work related purposes. Use of personal devices to access the network or applications require prior approval by the division security officer. Detection or incidents occurring through unauthorized use of personal devices will result in immediate NCID revocation;
- Have prohibited personal devices on agency property for the purpose of conducting non work-related activities and/or activities that have not been approved in advance by management. Prohibited personal devices without prior approval include thumb drives, electronic notebooks, tablets, or laptops. Divisions and Offices shall be responsible for enforcing policies and procedures on the approved use of voice or camera recording capabilities.
- Attempt to disguise their identity, the identity of their account or the resource that they are using. Users may not attempt to impersonate another person (i.e. use another individual's account) or organization. Likewise, users shall not misuse or misrepresent the department's name, resource names, or network address spaces;
- Attempt to intercept, monitor (i.e. read), forge, alter (i.e. change) or destroy (i.e. delete) another User's communications without express written permission from the Department CISO;
- Use resources in a way that disrupts or adversely impacts (degrades performance of) their legitimate uses or creates interference with/for other users. Such conduct includes, but is not limited to: hacking; illegal peer-to-peer file sharing; unauthorized alteration of resources that are likely to result in the loss of work, resource downtime; or excessive consumption resulting in congestion that interferes with the work of others;
- Use resources in an unlawful or illegal manner, including but not limited to; cyberstalking; threats of violence; obscenity (as described in NC General Statute (GS) 14-190.1.); child pornography; or any form that would constitute a criminal offense, a civil liability, or violation of any applicable law. In addition, users may not intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene. This provision applies to any digital communication distributed or sent with or while using Department resources;
- Use resources for private business, commercial or political activities, fundraising, non-departmental advertising, or activity that is prohibited by the DHHS Division of Human Resources and Office of State Human Resources;
- Download, install or run security software or utilities that reveals weaknesses in resources (e.g. vulnerability scanning, port mapping, network-mapping, etc..); monitors or intercept communications (e.g. packet sniffers, keystroke loggers, etc.); or allows for the attempting to bypass security controls (e.g. password crackers, etc.) without express written permission from the Department CISO;
- Download, install or distribute software to state-owned devices without express written permission from the DHHS Division or Office Director;

- Knowingly take any action which has the likelihood of introducing any virus, Trojan, malware (spyware, bot, ransomware, etc.) or other harmful software onto Departmental resources; nor should action be taken to deliberately circumvent controls designed to prevent such threats;
- Attempt to access restricted resources or communications without authorization by the appropriate owner or administrator;
- Engage in the unauthorized copying, distributing, altering or translating of copyrighted or State-owned materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law;
- Use resources in a manner that allows for the unauthorized gathering, dissemination or disclosure of confidential data (social security numbers, Personally Identifiable Information (PII), credit card numbers, medical records, Federal Tax Information (FTI), etc.);
- Extend, modify or retransmit network resources beyond what has been configured accordingly by the state or department through the installation of software or hardware (e.g. switches, routers, wireless access points, etc.) without express written permission from the DHHS Division or Office Director;
- Connect personal devices to the State Network without express written permission from the DHHS Division or Office Director (this requirement does not apply to state-supplied "guest" Wi-Fi networks);
- Connect personally owned "smart" devices (thermostats, wearable tech, appliances) to the State Network;
- Share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes;
- Download State data to personally owned devices without express written permission from the DHHS Division or Office Director;
- Attempt to obtain extra resources beyond those allocated or circumvent information security measures;
- Use Robotic Process Automation (RPA) robots to access state network or applications.

5.2.5 Requirements

The followed requirements must be adhered too:

- All devices connected to the State Network must have updated malware/antivirus protection;
- Users must ensure all files downloaded from an external source to the State Network or any device connected to the State Network, including a diskette, compact disc (CD), USB flash drive, or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code;
- Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization;
- Users must ensure that the transmission or handling of personally identifiable information;
- (PII) or other sensitive data is encrypted or has adequate protection;
- Users accessing the State Network through a Local Area Network (LAN) must avoid unnecessary network traffic and interference with other users;
- Access to the Internet from state-owned, home based, devices must adhere to all acceptable use policies. Employees must not allow family members or other non-employees to access nonpublic accessible information systems.

5.2.6 User Privacy

All users of the department's information systems are advised that their use of these resources and certain communications may be subject to monitoring and filtering. The Department reserves the right to monitor – randomly or systematically – the use of Internet and DHHS information systems connections and traffic. Any activity conducted using the state's information systems (including but not limited to computers, networks, e-mail, etc.) may be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable departmental policies and state and federal laws or rules. The department reserves the right to perform these actions with or without specific notice to the user.

5.2.7 Software License Agreements

All computer software, including software obtained from sources outside the department, is subject to license agreements that may restrict the user's right to copy and use the software. Software distributed on a trial basis, even via the Internet, does not suggest that the software is free or that it may be distributed freely.

The theft of software is illegal. The department does not require, request, or condone unauthorized use of software by its employees, volunteers, and contractors. The department enforces Federal Public Law 102-561, which strictly prohibits any violation of copyright protection. Violation of copyright protection is considered a felony and is punishable by up to five (5) years in prison and/or fines up to $250,000 for all parties involved.

DHHS information system hardware and software installations and alterations are handled by authorized DHHS employees or contractors only. Users shall not install new or make changes to existing software unless specifically approved by the User's supervisor and the designated IT personnel.

Downloading audio or video stream for a work-related webinar or audio conference is permissible without prior authorization, provided it is limited to the minimum amount of time necessary.

Figure 1. Workforce User Certification of Notification and Agreement of Computer Use Policy

USER CERTIFICATION OF NOTIFICATION AND AGREEMENT OF COMPUTER USE POLICY

I certify that I am an employee, volunteer, guest, vendor or contractor working for or on behalf of the Department of Health and Human Services and that I have read this "Acceptable Use Policy" and understand my obligations as described herein. I understand that this policy was approved by the Secretary of the Department of Health and Human Services and these obligations are not specific to any individual division or office of the department, but are applicable to all employees, volunteers, and contractors of the department. I understand that failure to observe and abide by these obligations may result in disciplinary action, which may include dismissal and/or contract termination. I also understand that in some cases, failure to observe and abide by these obligations may result in criminal or other legal actions. Furthermore, I have been informed that the department will retain this signed agreement on file for future reference. A copy of this agreement shall be maintained in the personnel file and/or in the contract administration file.

_____

Print Name

_____ _____

Employee, Volunteer, Guest, Vendor or Contractor Signature Date

_____ _____

Supervisor's Signature Date

5.3 ZixMail Usage Policy

This policy provides the framework for the usage of ZixMail within the Department to ensure compliance with HIPAA and other federal, department and state regulations and standards.

Guidelines

Sensitive data, internal proprietary and confidential data must be secured using approved encryption technologies when transmitted electronically. The Department intends ZixMail to be used for sending emails that contain sensitive and/or confidential information.

ZixMail is the email encryption tool employed by NC DHHS to ensure that official email communication containing confidential and/or sensitive information is secure and encrypted end-to-end between the sender an intended recipient(s). Confidential data includes, but is not limited to:

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Internal Revenue Service (IRS) data
- Payment Card Industry (PCI)
- Internal proprietary documents
- Trade secrets, design documents.

The primary purpose of email is to accomplish day to day Departmental business (general, operational, programmatic, and administrative). All emails sent via the NC Email system are subject to Public Records Requests, so personal or non-business-related communications should not be sent using the department email system. To facilitate the integrity and confidentiality of an email and its attachments, ZixMail must be used. ZixMail ensures the data is protected end-to-end in transit, meets federal, state and department requirements, and protects the integrity of data and emails for any public records requests.

There can be instances where it is determined that, due to the sensitivity of the data, email may not be an appropriate method used to transmit highly sensitive data. This can include IT system development code, application deployment/system testing, program/system certification, etc. In these instances, alternative communication channels should be used which can include, but would not be limited to alternative channels that:

- have specific communication capabilities such as web portals;
- use Secure File Transfer Protocol (SFTP) that meets state and federal encryption and password requirements

When the state and vendors agree that communication related to these types of contracts/agreements is specific and sensitive enough to establish alternative channels, these alternative channels must be used rather than department email.

Ch. 6. Breach and Complaints

6.1 HIPAA Breach Notification of Unsecured PHI

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted on February 17, 2009. Subtitle D of Division A of the HITECH Act, entitled ‘‘Privacy,’’ among other provisions, requires covered entities under HIPAA and their business associates to provide notification in the event of breaches of unsecured PHI as specified in HIPAA, 45 C.F.R. § 164.404. These notification requirements apply with respect to breaches of unsecured PHI occurring on or after September 23, 2009.

Guidelines

The Department HIPAA-covered components shall determine if an unauthorized acquisition, access, use, or disclosure of PHI is a “breach” that poses a significant risk of financial, reputational or other harm to the affected individual(s). In performing a risk assessment, DHHS Divisions and Offices must do the following:

- Determine whether PHI was involved;
- Determine whether there has been an unauthorized acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule;
- Determine, and document, whether the unauthorized acquisition, access, use or disclosure compromises the security or privacy of the PHI. Compromising the security or privacy of PHI occurs when there is a significant risk of financial, reputational, or other harm to the individual;
- Determine whether there was unsecured PHI involved in the breach (**i.e., not encrypted or destroyed**); and
- Determine whether an exception to the notification requirement applies.

6.1.1 Administrative Requirements

Training
DHHS Divisions and Offices covered by HIPAA shall train all members of their workforce with respect to breach reporting obligations and procedures, annually, so they are able to identify suspected breaches of unsecured PHI and know how to report all suspected breaches to their Privacy Official immediately. Evidence of employees receiving this annual training shall be documented and maintained.

Intimidating or Retaliatory Acts
DHHS Divisions and Offices are prohibited from retaliating against individuals who exercise their rights or file a complaint under the applicable HHS regulations.

Sanctions
Sanctions will be imposed upon members of the DHHS workforce who fail to comply with DHHS breach notification policies and procedures. DHHS expects that all employees will comply with all laws, regulations, standards, policies, procedures, guidelines and expectations regarding the privacy and security of DHHS protected health information. Violations of this policy may subject an employee to disciplinary action up to and including dismissal, as well as any potential civil or criminal sanctions under the law.

Filing of a Complaint
Individuals can file a complaint regarding a DHHS Division and Offices compliance with the HIPAA breach reporting rules. This complaint should be investigated and resolved in the same time frame and manner as other privacy complaints.

6.1.2 Reporting HIPAA Incidents and Complaints

DHHS Divisions and Offices should follow the procedures provided when they evaluate and report a suspected or known unauthorized acquisition, access, use, or disclosure of protected health information (PHI). These procedures will include information about to whom an impermissible acquisition, access, use, or disclosure of PHI should be immediately reported; who should be involved in determining if a breach of unsecured PHI has occurred; and if the affected individual(s) should be notified.

HIPAA-covered DHHS agencies which become aware of a suspected or known unauthorized acquisition, access, use, or disclosure of PHI shall **immediately** notify the DHHS Privacy and Security Office (PSO) by reporting the incident or complaint to the following link: https://security.ncdhhs.gov/

No later than five (**5**) business days, the DHHS Division or Office Privacy Official shall complete the **"Risk Assessment"** form that is located on a tab in the ticket reporting system. The questions on the risk assessment include such items as:

- Was PHI involved;
- If so, what types of PHI were involved;
- Was there an unauthorized acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule;
- Was the PHI encrypted using at least 128-bit encryption or destroyed by an acceptable method of destruction;
- Did the incident or complaint pose a significant risk of financial, reputational, or other harm to the individual;
- Does an exception to the notification requirement exist; and does the affected individuals need to be notified?

When information is not readily available for completion of the risk assessment, the DHHS Division or Office Privacy Official shall report the incident or complaint to the DHHS Privacy and Security Office (PSO) and use the ticket tracking ID number to update the incident or complaint as information becomes available.

Note*: Reporting to the DHHS PSO shall not be delayed for investigative reasons. If definite answers to all of the questions above are not available at the time the incident or complaint is reported, the DHHS Division and Office Privacy Official shall provide the remaining answers no later than five (5) business days after the event has been reported to the DHHS PSO.*

6.1.3 Review by DHHS PSO and DHHS Office of General Counsel

If the DHHS PSO determines that there may have been a breach of unsecured PHI, the DHHS PSO shall refer the event to DHHS General Counsel to make the final determination of whether a breach of unsecured PHI has occurred. If DHHS General Counsel, with assistance from the DHHS PSO and DHHS Division and Office staff, determines that a breach of unsecured PHI has occurred, the DHHS General Counsel shall recommend notification. To ensure sufficient time for DHHS staff to perform the evaluative process, and to prepare and coordinate notification, if required, the DHHS General Counsel shall make a final decision no later than forty-five (45) days after the department's discovery of the incident.

In order to determine whether the breach of unsecured PHI may require a press release, the DHHS PSO or the DHHS General Counsel shall consult with the Secretary and the DHHS Office of Public Affairs.

6.1.4 Evaluating a HIPAA Incident or Complaint

The reporting obligation for DHHS Divisions and Offices is triggered when there is a breach of unsecured PHI. In order to have a breach of unsecured PHI, there must be all of the following:

- PHI,
- Violation of the HIPAA Privacy Rule,
- Compromise of the privacy and security of the PHI,
- Unsecured PHI, and
- No exceptions.

PHI Involved

First, DHHS Divisions and Offices should always determine whether PHI was involved. If no PHI was involved, then there can be no breach of unsecured PHI and no obligation to notify.

Violation of the HIPAA Privacy Rule

DHHS Divisions and Offices must determine whether there has been an unauthorized acquisition, access, use, or disclosure of PHI in violation of the HIPAA Privacy Rule. If the DHHS Divisions and Offices determines that the HIPAA violation compromised the privacy and the security of the PHI, then the violation would be a "breach."

Limited data set + removal of dates of birth and zip codes

DHHS Divisions and Offices must determine whether a limited data set was involved or whether the dates of birth and zip codes had been removed. Disclosures of PHI that do not include an individual's date of birth or zip code and that meet the requirements of a limited data set are deemed not to compromise the security or privacy of PHI. Therefore, there would be no "breach" and notification would not be required.

Note: *If either zip codes or dates of birth are included in the limited data set, however, then DHHS Divisions and Offices would have to determine whether the incident compromised the privacy and security of the PHI.*

Compromises the privacy and security of PHI

If a DHHS Division and Office determines that there was a violation of the HIPAA Privacy Rule, it must determine whether the incident compromised the privacy or security of the PHI. The following 4 risk factors must be considered to determine if PHI has been compromised:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed;
- The extent to which the risk to the protected health information has been mitigated.

Unsecured PHI – Use of Encryption or Destruction

The term unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by HHS. On April 17, 2009, HHS issued guidance identifying two methods for "securing" PHI: encryption and destruction.

- **Encryption.** To be considered unreadable, PHI must be encrypted using an NIST approved algorithm and procedure. Electronic PHI is encrypted when the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and the key to decrypt the PHI was not obtained. It is important to note that in order to comply with the encryption standards and ensure the encryption keys are not obtained, DHHS Divisions and Offices must keep encryption keys on a separate device from the data that they encrypt or decrypt.
- **Destruction.** Destruction is also an acceptable method of rendering PHI unreadable. Paper, film, or other hard copy media should be shredded or destroyed such that the PHI cannot be read or otherwise reconstructed. Electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Exceptions to the Breach Notification Requirement

If DHHS Divisions and Offices determine that there was a breach of unsecured PHI, they must determine if an exception exists, which could either prevent the necessity for notification of affected individuals or delay notification. The exceptions are as follows:

- **Certain unintentional uses**. Notification is not required for any unintentional use, access, or acquisition of PHI by a DHHS workforce member or an individual acting under the authority of a DHHS Divisions and Offices or business associate, if the acquisition, access or use was made in good faith, within the scope of authority and does not result in further use or disclosure not permitted under the HIPAA Privacy Rule. For example, notification may not be required when a billing employee at a hospital mistakenly receives an email containing PHI, immediately deletes the email and alerts the sender of the mistake.
- **Certain inadvertent disclosures**. Notification is not required for any inadvertent disclosure of PHI by a person who is **authorized** to access PHI at a DHHS Divisions and Offices or business associate if the recipient is **authorized** to access PHI at the same DHHS Divisions and Offices, business associate or organized health care arrangement, and the disclosed PHI is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule. For example, notification may not be required when an employee misdirects an email the wrong employee, but the wrong employee is authorized to see the PHI.
- **Incidents involving no ability to retain the PHI**. Notification is not required when the DHHS Divisions and Offices or business associate has a good faith belief that the recipient was not reasonably able to retain the PHI. According to the federal Department of Health and Human Services (HHS), an example of this situation would be a covered entity that mails a number of explanations of benefits ("EOBs") to the wrong individuals, but the EOBs are returned unopened by the post office as undeliverable.
- **Law Enforcement Notification Delay Allowed**. DHHS Divisions and Offices are allowed to delay notification of affected individuals when law enforcement determines that there is a criminal investigation or that notification may damage national security.

  Note: *In this specific case, notification is still required.*

  If a law enforcement official informs the DHHS Divisions and Offices that the notice to individuals, to HHS or the media would impede a criminal investigation or cause damage to national security, the DHHS Divisions and Offices shall request that the law enforcement official make an official written request for the delay, specifying the following information:
    - his or her full name,
    - title,
    - organization name,
    - reason for the delay; and
    - proposed number of days to delay.

  All oral requests for a notification delay should be evaluated on a case by case basis. Oral requests for a notification delay should be granted only in the most urgent and serious circumstances. The law enforcement official is still required to provide the information above.

  DHHS General Counsel shall make the final determination of whether notification will be delayed. DHHS General Counsel may delay notification for up to thirty (30) days from the date the request was approved. If the law enforcement official can provide sufficient reasons for delaying notification more than thirty (30) days, DHHS General Counsel may consider his or her request.

6.1.5 Notification

If DHHS General Counsel determines that a breach of unsecured PHI has occurred, the DHHS Divisions and Offices shall provide notice of the breach and maintain documentation of such notice.

Guidance:

- **Notice to Affected Individual.** A written notice of breach shall be provided to each affected individual whose unsecured PHI has been breached, or is reasonably believed to have been breached, as follows:
  - **Timing of Notice**. The notice shall be provided promptly and no later than sixty (60) days after the DHHS Divisions and Offices discovers the breach. The breach is considered to be discovered on the first day on which the breach is known, or would have been known to any person who is a workforce member or agent of the DHHS Divisions and Offices (other than the person committing the breach) by exercising reasonable diligence.
  - **Manner of Notice**. The notice shall be sent by first-class mail addressed to the affected individual's last known address. Notice may be sent electronically if the individual has agreed to receive electronic notice and the agreement has not been withdrawn. If the DHHS Divisions and Offices **knows** that the individual is deceased, the DHHS Divisions and Offices shall provide written notice to the next-of-kin or personal representative of such individual if it has the addresses of those individuals. Notice may be provided in one or more mailings as additional information becomes available.
  - **Content of Notice**. The notice shall be written in plain language and shall contain the following information: (a) a brief description of the incident, including the date of the breach and the date of the discovery of the breach, if known, (b) a description of the types of unsecured PHI involved in the breach (rather than a description of the specific PHI), (c) any steps the individual should take to protect himself or herself from harm resulting from the breach, (d) a brief description of what the DHHS Divisions and Offices is doing to investigate the breach, to mitigate the harm to the individual and to protect against future occurrences, and (e) contact procedures for the individual to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website or postal address.
  - **Substitute Notice**. If there is insufficient or out-of-date contact information for an individual that precludes written notice to such individual, as soon as reasonably possible after such determination, the DHHS Divisions and Offices shall provide notice reasonably calculated to reach the individual as described below.
    - If there is insufficient or out-of-date contact information for **fewer than ten (10)** individuals, notice may be provided by e-mail, telephone or other means.

        - If there is insufficient or out-of-date contact information for **ten (10) or more** individuals, notice shall (1) be in the form of either a conspicuous posting for ninety (90) days on the DHHS main website home page or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside, and (2) include a toll-free number that remains active for at least ninety (90) days so that the individual can learn whether his or her unsecured PHI was included in the breach.
        - Substitute notice need not be provided if the affected individual is deceased and the DHHS Divisions and Offices has insufficient or out-of-date contact information for the next of kin or personal representative of the individual.
    - **Urgent Notice**. If the DHHS Divisions and Offices determines that there is potential for imminent misuse of the unsecured PHI in connection with a breach, the DHHS Divisions and Offices may provide information regarding the breach to individuals by telephone or other means, as appropriate, **in addition** to providing the required written notice as described above.

- **Notice to HHS.** The DHHS PSO also shall notify HHS of the breach of unsecured PHI. Such notification shall be provided as follows:
    - If the breach involves **500 or more** individuals, the DHHS PSO shall notify HHS of the breach contemporaneously with providing the notice to the individual and in a manner specified by HHS on its website.
    - If the breach involves **less than 500** individuals, the DHHS PSO shall maintain a log or similar documentation of the breach of unsecured PHI and shall report the required information on the HHS website no later than February 25th of each year.

- **Notice to Media**. If a breach involves **more than 500 residents of one state or jurisdiction**, in addition to notifying the individual and HHS, the DHHS Divisions and Offices also shall notify prominent media outlets serving the state or jurisdiction. Such notice shall be provided promptly and in no case later than sixty (60) calendar days after discovery of the breach. The notice shall contain the same information included in the notice to the individual.

EXAMPLE: If a DHHS Divisions and Offices discovers a breach of 600 individuals, 200 of which reside in North Carolina, 200 of which reside in Virginia, and 200 of which reside in South Carolina, such a breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media. However, individual notification would be required, as would notification to the HHS because the breach involved a total of 500 or more individuals. Conversely, if a DHHS Divisions and Offices discovered a breach of unsecured protected health information involving 600 residents within the state of North Carolina and 600 residents of Virginia, notification must be provided to the individuals, to a prominent media outlet serving the state of North Carolina, to a prominent media outlet serving the Commonwealth of Virginia and to HHS.

- **Communications with the Media or Outside DHHS Divisions and Offices.** With the exception of the DHHS PSO, the DHHS Office of the General Counsel, and the DHHS Office of Public Affairs, DHHS employees **are not** authorized to speak on behalf of the department to media personnel or representatives of other outside DHHS Divisions and Offices concerning HIPAA breach of unsecured PHI incidents that have or have not been reported. If you need additional help in understanding the document indicated above, please contact the DHHS Office of Public Affairs at (919) 855-4840.

6.1.6 Retention of Breach Notice Documentation

DHHS Divisions and Offices shall record and maintain thorough records of all activities related to suspected and known HIPAA breach of unsecured PHI incidents and to the provision of notice to either individuals, HHS, or any communication from law enforcement related to the delayed notification, if applicable, for at least six (6) years from the date the incident was closed or notice was provided, whichever date is the latest.

6.1.7 Reporting of Incident to DHHS by Business Associate

HITECH created requirements that apply directly to a covered entity's business associates ("BA") in the event of a breach of unsecured PHI. HIPAA-covered DHHS Divisions and Offices enter into contracts with business associates to perform functions, activities, or services on DHHS Divisions and Offices' behalves. If in the performance of this function, activity, or service, an incident involving the DHHS Divisions and Offices' PHI occurs, the BA is required to do the following:

- **Notify the DHHS Divisions and Offices.** BA shall notify the DHHS Divisions and Offices immediately, but no later than 24 hours after discovery of an incident involving the DHHS Divisions and Offices' PHI. The BA shall conduct an investigation immediately and provides the DHHS Divisions and Offices with answers to the following questions:
    - Was PHI involved;
    - If so, what types of PHI were involved;
    - Was there an unauthorized acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule;
    - Was the PHI encrypted using at least 128-bit encryption or destroyed by an acceptable method of destruction;
    - Did the incident pose a significant risk of financial, reputational, or other harm to the individual;
    - Does an exception to the notification requirement exist; and
    - Determine if the affected individuals need to be notified.

- **The content of the notification.** Content of the notification to the DHHS Divisions and Offices must also include, to the extent possible:
    - The identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, breached, and;
    - Any other available information that the DHHS Divisions and Offices is required to include in its notification to the individual.

When information is not yet available, the BA shall report the incident to the DHHS Divisions and Offices and update immediately as information becomes available. Reporting the incident to the DHHS Divisions and Offices shall not be delayed by BA for investigative reasons. The following steps shall be taken:

- **Complete Risk Assessment.** After notifying the DHHS Divisions and Offices about the incident, DHHS Divisions and Offices should require that the BA complete a risk assessment immediately, but no later than five (5) business days, to determine whether there has been a "breach of unsecured PHI." If definite answers to all of the questions above are not available at the time the incident is reported, the BA shall provide the remaining answers as they become available. The burden to determine whether there is a risk of harm resulting from the breach is on the DHHS Divisions and Offices - not the BA. Therefore, a BA should not have the discretion to determine whether notification will occur.
- **Contract language.** HIPAA-covered DHHS Divisions and Offices shall include appropriate language in all contracts with BAs to reflect the BA's responsibilities to do the following:
    - notify the DHHS Divisions and Offices of incidents immediately, but no later than 24 hours;
    - provide detailed information (See section V(F)(1));
    - investigate the incident;
    - complete a risk assessment;
    - update the DHHS Divisions and Offices as more information becomes available; and
    - pay all costs of notification or provide the notification, at the discretion of the DHHS Divisions and Offices.
- **Notification**. When an incident is reported by a BA, HIPAA-covered DHHS Divisions and Offices, in consultation with the DHHS PSO and DHHS General Counsel, shall review information provided by the BA to determine whether notification is required. If there is disagreement between the DHHS Divisions and Offices and the BA, the Divisions and Offices' decision shall control since DHHS owns the data and is responsible for providing the notification as the covered entity.

6.1.8 Overlapping Incidents and Complaints

Overlapping may occur when DHHS Divisions and Offices have an event that could violate HIPAA, the NC Identity Theft Protection Act, DHHS policy, other state and federal regulations or a combination thereof. When evaluating incidents or complaints, the DHHS Divisions and Offices should consult with their privacy or security officials to determine which type of incident needs to be reported.

6.2 Privacy Incident and Complaint Reporting

This policy establishes requirements for reporting, documenting, and investigating incidents and complaints resulting from suspected violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the North Carolina (NC) Identity Theft Protection Act, or the department's privacy practices, policies or procedures regarding confidential information.

Guidelines

Departments and Offices shall immediately report, investigate, and document all suspected privacy incidents or complaints electronically, ensuring that all required documents are attached to the electronic report. DHHS Divisions and Offices may report incidents or complaints using the DHHS Privacy and Security Office Incident Reporting Form or DHHS Privacy Complaint Report Form to document the incident or complaint and retain these documents for future reference. It is not necessary to attach these documents to the electronic report, however.

DHHS Divisions and Offices shall develop procedures to respond to incidents or complaints whenever there is reason to believe that their privacy practices, policies or procedures have been breached. Privacy incidents or complaints shall be resolved in a timely manner, ensuring clients and other individuals that the department is committed to protecting their confidential information. At a minimum, the following procedures shall be followed:

- DHHS Divisions and Offices shall designate a staff member who is responsible for communicating and assisting workforce members or individuals who have questions or concerns, or who wish to file incidents or complaints regarding the DHHS Division or Office privacy practices.
- When reporting incidents or complaints electronically, the DHHS Division or Office shall report its internal incident or complaint number, incident classification and severity, investigative analysis of the facts, description of the corrective actions taken, and mitigation efforts undertaken.
- The report shall be updated using the ticket tracking ID number, which is generated after submitting the incident or complaint until the investigation is completed and closed. In addition, any privacy incident or complaint that includes a disclosure for which an accounting is required must be documented and entered the accounting of disclosures logs.
- Respond to individuals who make inquiries, express concerns, and/or file complaints regarding the DHHS Division and Office privacy practices, policies, and procedures. Such communications may be rendered:
    - In person;
    - In writing (letter/e-mail/fax); or by telephone.
- Documentation of privacy incidents or complaints, investigative efforts, and incident or complaint determinations are considered administrative information and shall be maintained in administrative files for at least six (10) years. Documentation of privacy incident or complaint information shall not be filed in a client's treatment, financial, or other designated record sets.

6.2.1 Reporting Incidents and Complaints

Guidance:	• **Communication Methods**
	  ○ **Incidents**: A DHHS workforce member, business associate or vendor shall report incidents to the DHHS Division and Office Privacy Official or Privacy Coordinator. The Privacy Official or Privacy Coordinator shall then report the incident to the DHHS PSO electronically.
	  ○ **Complaints**: An individual can file a complaint with the DHHS Division and Office directly, or with the department's Privacy Officer. The DHHS Privacy and Security Office is responsible for maintaining a current list of designated privacy contacts in each DHHS Division and Office and; therefore, each DHHS Division and Office is required to notify the

DHHS Privacy and Security Office of any staff changes in their privacy official or privacy coordinator positions.

- **DHHS Division and Office:** An individual may file a privacy complaint in person, in writing or by telephone directly with an DHHS Division and Office. The Privacy Official or Privacy Coordinator shall immediately notify the complainant in writing that the DHHS Division and Office has received his/her complaint, is investigating it and will notify the complainant of its resolution. DHHS agencies shall not retaliate against any individual for filing a HIPAA privacy complaint with either the DHHS Division and Office, the department, or the Secretary of the US Department of Health and Human Services
- **Department's privacy officer:** An individual may file a complaint with the DHHS Privacy and Security Office if, for some reason, the individual does not wish to speak to the DHHS Division and Office Privacy Official or Privacy Coordinator. Such communication may be accomplished in person, in writing, or by telephone. If an individual contacts the DHHS Privacy and Security Office before an DHHS Division and Office, the DHHS Privacy and Security Office shall determine if the issue is DHHS Division and Office-specific and shall attempt to refer the individual to the appropriate DHHS Division and Office, as needed. If the individual does not wish to speak with DHHS Division and Office staff directly, the DHHS Privacy and Security Office shall collect the complaint information and work with the DHHS Division and Office Privacy Official or Privacy Coordinator to resolve the issue.

6.2.2 Documenting, Investigating, and Resolving Incidents and Complaints:

Guidance:

- **Documentation**
  - All complaints can be entered into the incident reporting system. It is located at https://security.ncdhhs.gov/
  - The DHHS Division and Office shall document all telephone complaints and direct complainant to the Incident reporting site so that the event shall be investigated as an incident.

- **Investigation and Resolution**
  - Investigation of privacy incidents or complaints must begin immediately following receipt of an expressed incident or complaint. Investigative actions and resolution shall be documented electronically using the link https://security.ncdhhs.gov/ .
  - Once a ticket is entered into the incident reporting system, the appropriate privacy or security official is assigned to investigate the allegation. It is important to provide detailed information, including dates, locations, titles, types of identifiers involved and attach documents, since this will be the DHHS Division and Office main record of the investigation.

- **Responsibility of Privacy Official or Privacy Coordinator**
  - Each DHHS Division and Office shall determine its procedures for investigating and resolving privacy incidents or complaints. However, each DHHS Division and Office must designate an individual as Privacy Official (if covered by HIPAA) and/or as Privacy Coordinator (if not covered by HIPAA), who will be responsible for reporting, investigating and documenting privacy incidents or complaints.
  - If an individual reaches out to the DHHS Division and Office directly, the DHHS Division and Office Privacy Official or Privacy Coordinator shall determine if the issue can be resolved at the DHHS Division and Office level. If so, the Privacy Official or Privacy Coordinator shall be responsible for investigating and documenting the concern until the issue is resolved. Agencies operated by the Division of State Operated Healthcare Facilities are encouraged

to involve their internal client advocates in the complaint investigation process when deemed appropriate.
  - If the Privacy Official or Privacy Coordinator determines the issue involves other agencies in the department or if he/she is unable to obtain resolution at the DHHS Division and Office level, the issue shall be forwarded to the DHHS Privacy and Security Office.

- **DHHS Privacy and Security Office Review**
  - The DHHS Privacy and Security Office shall review the reporting, documentation and resolution of all privacy incidents or complaints. If the DHHS Division and Office has not resolved the incident within a reasonable time, the DHHS Privacy and Security Office shall involve anyone determined to be necessary to assist in resolution of the incident or complaint, including the Attorney General's Office. If the DHHS Privacy and Security Office has comments, suggestions, questions, etc. about the investigation and resolution of the incident or complaint, he or she shall document this information within the report for consideration by the DHHS Division and Office.

- **Training**
  - Whenever a privacy incident or complaint has occurred, the DHHS Division and Office must evaluate the occurrence to determine if additional staff training is necessary. Depending upon the situation, it may be determined that the entire DHHS Division and Office should receive training that is specific to the privacy incident or complaint. The Privacy Official or Privacy Coordinator shall review any privacy training developed as part of the privacy incident or complaint resolution to ensure the scope of the training adequately addresses the subject of the incident and reinforces the Department and DHHS Division and Office privacy practices, policies and procedures.

6.2.3 Types of Incidents and Complaints

For purposes of this policy, there are three types of privacy incidents or complaints: HIPAA, NC identity theft, and departmental practice, policy or procedure violations. There may be times when these three types of privacy incidents or complaints overlap, and agencies are unsure about whether any given event could be considered a breach of unsecured PHI, a security breach, a departmental practice, policy or procedure violation, or a combination thereof. In these instances, please contact the DHHS Privacy and Security Office for guidance.

HIPAA incidents and complaints (breach of unsecured PHI)

- The **HIPAA Breach Notification for Unsecured PHI policy** outlines the procedures HIPAA covered DHHS agencies should follow when they evaluate and report an unauthorized acquisition, access, use, or disclosure of protected health information (PHI). These procedures include information about to whom an impermissible acquisition, access, use, or disclosure of PHI should be immediately reported, who should be involved in determining if a breach of unsecured PHI has occurred and if the affected individual(s) should be notified.
- HIPAA covered agencies which become aware of an unauthorized acquisition, access, use, or disclosure of PHI shall **immediately** notify the DHHS Privacy and Security Office (PSO) by reporting the incident or complaint to the following link: https://security.ncdhhs.gov/ and complete the applicable sections .

NC Identity Theft Protection Act incidents and complaints (security breach)

- The **Identity Theft and Security Breach Notification policy** outlines the procedures all DHHS agencies should follow when they report a disclosure or possible disclosure of identifying information. These procedures will include information to whom a disclosure or possible disclosure of identifying information should be immediately reported; who should be involved in determining if a security breach has occurred and if the affected persons should be notified. Any DHHS Division and Office which becomes aware of a disclosure or possible disclosure of identifying information shall **immediately** notify the DHHS PSO by reporting the incident or complaint to the following link: https://security.ncdhhs.gov/ and complete the applicable sections.

Departmental policy or procedure violation incidents or complaints.

- There are DHHS Divisions and Offices that maintain confidential information but are not covered by HIPAA. The Privacy Safeguards policy specifically addresses how DHHS Divisions and Offices should protect confidential information from unauthorized use or disclosure.
- Any DHHS Division and Office which becomes aware of an unauthorized use or disclosure of confidential information shall **immediately** notify the DHHS PSO by reporting the incident or complaint to https://security.ncdhhs.gov/.

Ch. 7 Identity Theft Policies

7.1 Identity Theft Red Flags and Address Discrepancy Policy

The Fair and Accurate Credit Transactions Act of 2003, is also known as the Red Flag and Address Discrepancy Rules. The policy shall apply to the requirements of this regulation.

Guidance

DHHS Divisions and Offices shall develop and implement specific policy and procedures to support the department's Identity Theft Prevention Program by identifying, preventing and mitigating any evidence of theft that arises during business. This policy shall also apply to divisions and offices that issue debt/credit cards or utilize consumer reports when extending credit.

Financial Institution Operations:
Divisions shall determine whether it must comply with this policy based on whether they operate as a financial institution, creditor that offers or maintains covered accounts and/or a debit/credit card issuer. If the DHHS Division and Office determines that it meets the definition of a financial institution, it must perform a risk assessment and develop required policies and procedures.

7.1.1 Red Flag and Address Discrepancy Policy

For a DHHS Division or Office to determine whether the Red Flag and Address Discrepancy Rules applies to its business operations, the DHHS Division and Office should perform a risk assessment.

If the DHHS Division or Office determines that it operates as a financial institution or a creditor that owns or maintains covered accounts, it must develop and implement reasonable procedures to detect, prevent, and mitigate identity theft as part of the department's *Identity Theft and Prevention Program.*

7.1.2 Financial Institution or a Creditor That Owns or Maintains Covered Accounts

If the DHHS Division or Office determines that it operates as a financial institution or a creditor that owns or maintains covered accounts, it must develop and implement reasonable procedures to detect, prevent and mitigate identity theft as part of the department's *Identity Theft Prevention Program*.

7.1.3 Debit/Credit Card Issuer

If the DHHS Division or Office determines that it issues debit or credit cards, it must develop procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. These procedures will be incorporated into the department's Identity Theft Prevention Program.

7.1.4 User of a Consumer Report

If the DHHS Division and Office determines that it uses consumer reports as part of its business operations, it must develop procedures to respond to a notice of address discrepancy received from a consumer reporting agency. These procedures will be incorporated into the department's Identity Theft Prevention Program.

7.1.5 Identity Theft Prevention Program

Those divisions and offices that are subject to the Red Flag and Address Discrepancy Rules will be required to perform the following functions as part of the DHHS Identity Theft Prevention Program:

- Identify their covered accounts;
- Identify their relevant red flags;
- Review/develop mechanisms to detect red flags;
- Review/develop mechanisms to prevent, mitigate, and respond to identity theft incidents;
- Add the Red Flag and Address Discrepancy Rules' requirements to their current identity theft compliance program activities;
- Ensure Service Providers' compliance with the Red Flag and Address Discrepancy Rules (covered accounts, transaction accounts, or debit/credit cards);
- Provide employee training; and
- Provide oversight of and review its procedures for effectiveness.

The Red Flags Rule sets out how certain businesses and organizations must develop, implement, administer and oversee their Identity Theft Prevention Program. The Program must include four basic elements, which together create a framework to address the threat of identity theft. The purpose of the Identity Theft Prevention Program is to detect, prevent, and mitigate identity theft in connection with new or existing covered accounts. It must be appropriate to the **size, complexity, nature,** and **scope** of the department's activities.

- **Elements of the Program.**
    - **Policies and Procedures.** The department's Program must include policies and procedures to identify the "red flags" of identity theft that a DHHS Division and Office may run across in the day-to-day operations of its business. For example, if a customer must provide some form of identification to open an account, an ID that looks like it might be fake would be a "red flag" for a DHHS Division and Office.
    - **Detection.** The Program must be designed to detect the red flags the DHHS Division and Office has identified. For example, if a DHHS Division and Office has identified fake IDs as a red flag, it must have procedures in place to detect possible fake, forged or altered identification.
    - **Response**. Program must spell out appropriate actions the DHHS Division and Office will take when it detects red flags.
    - **Evaluation.** The DHHS Division and Office must address how it will re-evaluate its Program periodically to reflect new risks from this crime.

If a DHHS Division and Office issues debit and/or credit cards or uses consumer reports, the Program will also include procedures to:

- Assess the validity of a change of address for a debit or credit card account if an individual request an additional or replacement card for the same account shortly thereafter; and/or
- Enable the recipient or a credit report, after receiving a notice of address discrepancy, to form a reasonable belief that a consumer's address has changed and to provide the reasonably confirmed address to the consumer reporting agency from whom it received the notice of address discrepancy.

- **Administration of the Program**.
  DHHS provides for the continued administration of the *Identity Theft Prevention Program* by ensuring divisions and offices perform the following:
    - **Obtaining** approval of the initial written Program from either the Secretary of DHHS (Secretary) or his or her designee;
    - **Reporting to the Secretary** on exceptions, risks, and Program effectiveness;
    - **Detecting, logging,** and **resolving** identified Red Flag exceptions;
    - **Training management** and **staff** to effectively implement the divisions' and offices' procedures;
    - **Exercising** effective oversight of Service Providers and binding them to compliance via contract;
    - **Considering** the guidelines in Appendix B and **including** those guidelines that are appropriate in its procedures; and
    - **Periodically monitoring** the divisions' and offices' procedures for changes in scope--which could include new covered accounts or red flags--legislation, and effectiveness.

- **Guidelines for Formulating and Maintaining an Identity Theft Prevention Program:**
    - **Detecting Red Flags**. When the DHHS Division and Office performs a risk assessment and determines that it is subject to Red Flag Rule compliance, the division's or office's procedures should, at a minimum, address the detection of Red Flags in connection with the opening of covered accounts and with existing covered accounts, such as by:

        - Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
        - Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

    - The procedures should include relevant Red Flags from the following five categories:
        - Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
        - The presentation of suspicious documents;
        - The presentation of suspicious personal identifying information, such as a suspicious address change;
        - The unusual use of, or other suspicious activity related to, a covered account; and
        - Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

    - **Preventing, Mitigating, and Responding to Identity Theft Incidents**. The division's or office's procedures should provide for appropriate responses to the red flags it has detected that are commensurate with the degree of risk posed. In determining an appropriate response, the DHHS Division and Office should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a client's account records held by the DHHS Division and Office or third party, or notice that a client has provided information related to a covered account held by the DHHS Division and Office to someone fraudulently claiming to represent the DHHS Division and Office or to a fraudulent website. Appropriate responses may include the following:
        - Monitoring a covered account for evidence of identity theft;
        - Contacting the customer;
        - Changing any passwords, security codes, or other security devices that permit access to a covered account;
        - Reopening a covered account with a new account number;
        - Not opening a new covered account;
        - Closing an existing covered account;
        - Not attempting to collect on a covered account or not selling a covered account to a debt collector;
        - Notifying law enforcement; or
        - Determining that no response is warranted under the circumstances.

    - **Debit/Credit Card Issuers**. A DHHS Division and Office that issues debit or credit cards must establish and implement reasonable policies and procedures to assess the validity of a change of address if it:
        - Receives notification of a change of address for a consumer's debit or credit card account; and
        - Within a short period of time afterwards (during at least the first 30 days), the DHHS Division and Office receives a request for an additional or replacement card for the same account.

    Under these circumstances, the DHHS Division and Office is not allowed to issue an additional or replacement card, until:
        - The cardholder is notified of the request:
        - At the cardholder's former address; or
        - By any other means of communication, the DHHS Division and Office and the cardholder have previously agreed to use; and
        - The cardholder is provided a reasonable means of promptly reporting incorrect address changes.

- **Oversight, Development, Implementation and Administration of the DHHS Identity Theft Program.** The Secretary of DHHS shall be responsible for designating an employee at the level of senior management to oversee the DHHS Identity Theft Program and assigning specific responsibility for the Program's implementation within the department.

7.2 Identity Theft and Security Breach Notification

The North Carolina (NC) General Assembly enacted the NC Identity Theft Protection Act which became effective on December 1, 2005. The Identity Theft Act protects Social Security Numbers (SSN's) and other identifying information that DHHS receives, collects, uses, stores, discloses and mails in compliance with North Carolina General Statutes (N.C.G.S.) § 132-1.10. The Security Breach

Notification policy outlines procedures for responding to a security breach involving the unauthorized disclosure of unencrypted personal information, in compliance with N.C.G.S. § 132-1.10(c1) and N.C.G.S. § 75-65.

The Security Breach Notification policy outlines procedures for responding to a security breach involving the unauthorized disclosure of unencrypted personal information, in compliance with N.C.G.S. § 132-1.10(c1) and N.C.G.S. § 75-65.

The DHHS policy shall provide direction regarding the collection, usage, storage, transmission, mailing, and disclosure of SSNs and other identifying information. The policy will specifically aim to increase DHHS workforce member awareness about the confidential nature of SSNs and other identifying information; the emphasis on the secure use, collection; the transmission and storage of SSNs and other identifying information; and the confidence of clients and workforce members on the confidential treatment of their SSN data.

Guidance

DHHS Divisions and Offices shall request an individual's identifying information only when required to do so by Federal or State laws and as necessary to conduct legitimate business operations. Where the purpose of the identifying information can be satisfied by another personal unique identifier, reduce the SSN to the last four digits or remove entirely.

7.2.1 Collection, Usage, Storage, Transmission, Mailing, Disclosure and Destruction

DHHS Divisions and Offices that maintain SSNs and other identifying information in paper form or electronic media shall adhere to the following procedures regarding its collection, usage, storage, transmission, mailing and disclosure, in compliance with N.C.G.S. § 132-1.10.

- **Collection:** DHHS Divisions and Offices shall not collect SSNs unless and until:
    - The collection is authorized by law or imperative for the performance of the DHHS Division and Office duties and responsibilities as prescribed by law;
    - The collection is relevant to the purpose for which it is collected;
    - The need for the collection has been clearly documented;
    - The SSNs have been segregated on a separate page, so they are easy to redact when there is a valid public records request; and;
    - A statement of the purpose(s) for which the SSN is being collected and used is provided to the individual, upon their request, at the time of **or** prior to the DHHS Division and Office actual collection of the SSN.

- **Usage:** DHHS Divisions and Offices shall not use SSNs for any purpose other than the purpose stated in this policy. Usage shall be for a legitimate business purpose, and a duty exists to safeguard this data and prevent unnecessary access thereto.

- **Storage:** DHHS Divisions and Offices shall first evaluate and determine whether there is a legitimate business need to store SSNs before this data can be stored in DHHS system applications, locked filed cabinets, or other storage containers. DHHS agencies should reduce the SSN to the last four (4) digits, whenever possible, or replace it with a random identification number. When storage of the entire SSN is necessary, DHHS agencies should implement appropriate safeguards to prevent the possibility of workforce member misuse.

- **Transmission:** DHHS Divisions and Offices shall not:
    - Require an individual to transmit an SSN over the Internet unless the connection is secure, **or** the SSN has been encrypted; or;
    - Require an individual to use an SSN to access an Internet web site unless a password, unique identification number or other authentication device is also required.

- **Mailing**: No DHHS Division and Office will:
    - Intentionally print or embed an SSN on any card required to access government services (i.e. Medicaid, food stamps, etc.);
    - Print an SSN on any mailed materials, unless state or federal law requires it;
    - If required, print an SSN (in whole or in part) on a postcard or other mailer not requiring an envelope;
    - Make an SSN visible on an envelope; or
    - Make an SSN visible without the envelope having been opened.

- **Disclosure:** DHHS Divisions and Offices may disclose SSNs, other identifying information or documents containing SSNs or other identifying information only in the following instances:
    - Disclose to another governmental entity or its agents, employees, or contractors if disclosure is necessary for the receiving entity to perform its duties and responsibilities.

      Note: *The receiving governmental entity and its agents, employees, and contractors shall maintain the confidentiality of this information.*

    - Disclose pursuant to a court order, warrant, or subpoena;
    - Disclose for public health purposes, pursuant to and in compliance with Chapter 130A;
    - Disclose documents where SSNs or other identifying information have been redacted;
    - Disclose SSNs or other identifying information on certified vital records issued by the NC State Registrar or authorized officials, pursuant to N.C.G.S. § 130A-93(c);
    - Disclose any identifying information, other than SSNs, on uncertified vital records; or
    - Disclose SSNs or other identifying information in a recorded document in the official records of the NC Register of Deeds office or in the Courts.

- **Destruction:** DHHS Divisions and Offices must take reasonable measures to protect SSNs, and personal information against unauthorized access to or use of the information in connection with or after its disposal. The reasonable measures may include:
    - The burning, pulverizing or shredding of papers containing SSNs or personal information so this information cannot be practicably read or reconstructed; or
    - The destruction or erasure of electronic media and other non-paper media containing SSNs or personal information so the information cannot practicably be read or reconstructed.

  DHHS Divisions and Offices may, after due diligence, enter a written contract with, and monitor compliance by, a third party engaged in the business of record destruction to destroy SSNs or personal information. Due diligence should ordinarily include one or more of the following:
    - Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review; or
    - Taking other appropriate measures to determine the competency and integrity of the disposal business.

  Note: *It is the department's preference that the record destruction company shred documents containing SSNs and other confidential information onsite at the DHHS Division and Office's location. Bear in mind that if any HIPAA data is being shred, a Business Associate Agreement must be in place with vendor.*

7.2.2 Security Breach

N.C.G.S. § 132-1.10(c1) states that "if an agency of the state or its political subdivisions, or any agency or employee of a government agency, experiences a security breach, as defined in Article 2A of Chapter 75 of the G.S., the agency shall comply with the requirements of N.C.G.S. § 75-65."

The NC General Assembly enacted N.C.G.S. § 75-65 to require "businesses" and state or local governments to give individuals early warning when their personal information has been accessed by an unauthorized person, so they can take steps to protect themselves against identity theft or to mitigate the crime's impact.

DHHS Divisions and Offices shall adhere to the following procedures when reporting a disclosure or possible disclosure of identifying information.

Guidance:	• **Reporting disclosures or possible disclosures involving identifying information:** Any DHHS Division or Office which becomes aware of a disclosure or possible disclosure of identifying information shall **immediately** report the privacy incident or complaint to the DHHS Privacy and Security Office (PSO) and provide answers to the following questions, if known: o What types of identifying information were involved (i.e. SSN, driver's license, etc.); o Was health or financial information involved;

- Was the individual's first name **or** first initial **and** last name included;
- Was the identifying information in electronic or paper form;
- Was the information or the laptop encrypted (128-bit encryption);
- Was the identifying information stolen, lost, misplaced or other; and
- Was the information disclosed to the public?

Note: *Reporting to the DHHS PSO shall not be delayed for investigative reasons. If definite answers to all of the questions above are not available at the time the disclosure or possible disclosure is immediately reported to the DHHS PSO, the DHHS Division and Office shall provide the remaining answers no later than three (5) business days after the event has been reported to the DHHS PSO.*

- **Privacy Official or Privacy Coordinator:** When a disclosure or possible disclosure of identifying information is suspected to have occurred, the Privacy Official or Privacy Coordinator will be charged with reporting to the DHHS PSO and coordinating the division or office's investigation. DHHS Divisions and Offices are encouraged to implement their own internal reporting and investigative procedures to ensure all essential personnel are included in the process and events are reported timely.

- **Evaluation and Response to reported disclosure:** Once reported, the DHHS PSO, in conjunction with the DHHS Division and Office Privacy Official or Privacy Coordinator and other necessary staff, will make an initial evaluation to determine the following:
  - If the disclosure or potential disclosure involved confidential information;
  - If the disclosure or potential disclosure involved protected health information or electronic protected health information; and
  - If the disclosure or potential disclosure involved unencrypted and unredacted records or data containing "personal information".

- **Reporting security incidents to the Office of DIT:** All security incidents must be reported to the Office of DIT. This reporting is handled by the Privacy and Security office. (See Statewide Information Security Manual, Chapter 13 - Detecting and Responding to ITS Incidents Standard, Section 01:130101 - Reporting Information Security Incidents). If you are unsure how to report the event, please contact the DHHS PSO for assistance.
  https://security.dhhs.state.nc.us/incidents/security/index.php

  Note: *Not all reported security incidents are found to be breaches after evaluation; however, all incidents MUST be reported to the PSO through the incident reporting tool.*

- **Reporting Disclosures or Potential Disclosures Involving PHI:** If a DHHS Division and Office is covered by HIPAA and determines that it has disclosed protected health information (PHI) or electronic protected health information (ePHI) without authorization, a HIPAA privacy incident should be reported, investigated and mitigated as required by the Privacy Incident and Complaint Reporting policy (See the HIPAA Breach Notification for Unsecured PHI policy).

- **Reporting Disclosures or Potential Disclosures Involving Unencrypted and Unredacted Records or Data containing Personal Information:** If, after making an initial evaluation, the DHHS PSO determines that there has been a disclosure or potential disclosure of unencrypted and unredacted records or data containing personal information, the DHHS PSO shall refer the event to the Office of General Counsel to determine whether a security breach has occurred. If the DHHS General Counsel, with assistance from the DHHS PSO and DHHS Division and Office staff, determines that a security breach has occurred, a decision regarding notification of affected persons will be made by the DHHS General Counsel without unreasonable delay.

  If it is determined that the security breach may require a press release, the DHHS PSO or the DHHS General Counsel shall notify the Deputy Secretary, the Director of the Office of Public

Affairs (PAO), and the DHHS Division and Office Director.

Note: *There may be instances when overlapping issues arise and DHHS agencies are unsure about whether any given event could be considered a security incident, a HIPAA Privacy incident, a security breach or a combination thereof. Open a ticket, PSO can make a final determination as to classification of an incident.*

7.2.3 Reporting of Incident by a Non-DHHS Organization

N.C.G.S. § 75-65(b) requires that a non-DHHS organization that maintains or possesses records that DHHS owns or licenses notify DHHS of any security breach immediately following discovery of the breach. DHHS Divisions and Offices enter contracts with other non-DHHS organizations to perform specific tasks, involving the non-DHHS organization's use of DHHS identifying information. If, in the performance of this contract, DHHS identifying information is lost, misused, disclosed without authorization, etc., the non-DHHS organization is required to do the following:

Guidance:

- Notify the DHHS Division and Office: The non-DHHS organization shall notify the DHHS Division and Office immediately, but no later than twenty-four (24) hours after discovery of an incident involving the DHHS Division and Office's identifying information. The DHHS Division and Office is required to notify affected persons without unreasonable delay. Therefore, it is imperative that the non-DHHS organization investigates immediately and provides the DHHS Division and Office with answers to the following questions:
    - What types of identifying information were involved (i.e. SSN, driver's license, etc.);
    - Was health or financial information involved;
    - Was the individual's first name **or** first initial **and** last name included;
    - Was the identifying information in electronic or paper form;
    - Was the information or the laptop encrypted (128-bit encryption);
    - Was the identifying information stolen, lost, misplaced or other; and
    - Was the information disclosed to the public?

There may be times when answers to the questions above are not yet available. In these instances, the non-DHHS organization shall report the incident to the DHHS Division and Office and update the DHHS Division and Office immediately as information becomes available. Reporting the incident to the DHHS Division and Office shall not be delayed by the non-DHHS organization for investigative reasons or contacting law enforcement.

7.2.4 Complete Risk Assessment

After notifying the DHHS Division and Office about the incident, DHHS agencies should require that the non-DHHS organization complete a risk assessment immediately, but no later than five (5) business days, to determine whether there has been a "security breach." If definite answers to all the questions above are not available at the time the incident is reported, the non-DHHS organization shall provide the remaining answers as they become available. The burden to determine whether there is a risk of harm resulting from the breach is on the DHHS Division and Office - not the non-DHHS organization. Therefore, a non-DHHS organization **should not** have the discretion to determine whether notification will occur.

Guidance:	• **Contract language:** DHHS Divisions and Offices shall include appropriate language in all contracts with non-DHHS organizations to reflect their responsibilities to do the following:
	  ○ notify the DHHS Division and Office of incidents immediately, but no later than 24 hours;
	  ○ investigate the incident;
	  ○ complete a risk assessment;
	  ○ update the DHHS Division and Office as more information becomes available; and
	  ○ pay all costs of notification or provide the notification, at the discretion of the DHHS Division and Office.
	
	• **Notification**: When an incident is reported by a non-DHHS organization, DHHS agencies, in consultation with the DHHS PSO and DHHS General Counsel, shall review information provided by the organization to determine whether notification is required. If there is disagreement between the DHHS Division and Office and the non-DHHS organization, the DHHS Division and Office's decision shall control when DHHS owns the identifying information and is responsible for providing the notification as the owner of the information.

7.2.5 Duty to Notify the Attorney General's Office

Although N.C.G.S. § 75-65 applies to a "business" and the definition of "business" excludes any government or governmental subdivision or agency, N.C.G.S. § 132-1.10(c1) specifically states that if an agency of the State or its political subdivisions, or any agent or employee of a government agency, experiences a security breach, the agency shall comply with the requirements of N.C.G.S. § 75-65. Accordingly, DHHS agencies are obligated to notify the Consumer Protection Division of the Attorney General's Office pursuant to N.C.G.S. § 75-65(e1), without unreasonable delay, when there is a security breach and notice to affected persons is required.

Guidance:	• DHHS Divisions and Offices shall notify the NC Attorney General's Office's at their Security Breach Reporting Information website and ensure that they include the following information in the form:
	  ○ Nature of the breach, o the number of consumers affected by the breach, o steps taken to investigate the breach,
	  ○ Steps taken to prevent a similar breach in the future, and
	  ○ information regarding the timing, distribution, and content of the notice
	
	DHHS General Counsel will notify or delegate the responsibility to notify the Consumer Protection Division of the NC Attorney General's Office.

7.2.6 Duty to Report to both the Attorney General's Office and Consumer Reporting Agencies.

N.C.G.S. § 75-65(f) requires that in the event DHHS provides notice of a security breach to more than 1,000 persons at one time, it shall notify, without unreasonable delay, the Consumer Protection Division of the NC Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. If more than 1,000 affected persons at one time must be notified, DHHS Divisions and Offices shall follow the procedure outlined in Section D above and report the security breach to the three credit reporting agencies, Equifax, TransUnion, and Experian.

- **Equifax**
  Equifax.com/personal/credit-report-services

800-685-1111
Equifax Complaint Department, P.O. Box 740241, Atlanta, GA 30374-0241

- **Experian**
  Experian.com/help
  888-EXPERIAN (888-397-3742)
  Experian National Consumer Assistance Center, P.O. Box 9532, Allen, TX 75013
- **Transunion**
  TransUnion.com/credit-help
  888-909-8872
  TransUnion Fraud Victim Assistance Department, P.O. Box 6790, Fullerton, CA 92634

7.2.7 Duty to Report to the General Assembly

N.C.G.S. § 120-270 requires all agencies of the state to evaluate and report to the General Assembly about the agency's efforts to reduce the dissemination of identifying information, as defined in N.C.G.S. § 14-113.20(b) by December 31st of each year. The evaluation should include a review of the agency's public forms, the use of its random personal identification numbers, the restriction of access to its personal identifying information, and the reduction of use of its personal identifying information when it is not necessary. Special attention should be given to the agency's use, collection, and dissemination of SSNs.

In order to ensure compliance with this statute, the DHHS PSO shall coordinate the evaluation and reporting of the department's efforts to reduce the dissemination of SSNs and other identifying information.

7.2.8 Communications with the Media or Outside Agencies

With the exception of the DHHS PSO, the Office of the General Counsel, and the NC Office of Public Affairs, DHHS workforce members **are not** authorized to speak on behalf of the department to media personnel or representatives of other outside agencies concerning privacy or security incidents that have or have not been reported. If you need additional help in understanding the document indicated above, please contact the NC Office of Public Affairs at (919) 855-4840.

-- End of Document –

Page intentionally left blank.

CHAPTER: NC DHHS Privacy Manual Updates

Policy Section	Review Mo/Yr.	Revision Mo/Yr.	Original Approved By	New/Revision Language
Ch. 5.2.4	6/2/2021	6/2/2021	Pyreddy Reddy/Sam Gibbs	• **New Language:** 5.2.4. Prohibited Uses. Users shall not: 1) Connect personal devices or equipment to the network or applications that contain confidential data for work related purposes. Use of personal devices to access the network or applications require prior approval by the division security officer. Detection or incidents occurring through unauthorized use of personal devices will result in immediate NCID revocation; 2) Have **prohibited** personal devices on agency property for the purpose of conducting non work-related activities and/or activities that have not been approved in advance by management. **Prohibited** personal devices without prior approval include thumb drives, electronic notebooks, tablets, or laptops. Divisions and Offices shall be responsible for enforcing policies and procedures on the approved use of voice or camera recording capabilities. 20.) Use Robotic Process Automation (RPA) robots to access state network or applications.