What is HIPAA?

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, is a federal law that:

- Provides Portability: Protects and guarantees health insurance coverage when an employee changes jobs

- Provides Accountability: Protects health data integrity, confidentiality, and availability

- Sets National Standards for Electronic Data Transmission
  - Transactions (eligibility, claims, payment, and others) and identifiers
  - Standard medical codes (e.g., ICD-9, CPT-4, no use of “local” codes)

- **Sets National Standards for the Protection of Health Information**
  - Privacy (operational, consumer control, administration)
  - Security (administrative, physical, technical, network)

Why Comply with HIPAA?

- Protecting the confidentiality of our clients' health information is critical to maintaining trust and confidence in the public health system.

- Protecting client health information
  - Is the right thing to do!
  - Is required by law!

Who is Covered by HIPAA?

- The organizations covered by HIPAA are defined as “covered entities.”
- Health Care Providers who conduct any of the HIPAA-regulated transactions electronically. The Health Services Information System (HSIS) provides billing services for local health departments, State Lab, and Child Development Service Agencies (CDSAs), formally called the DECs, and submits claims electronically to Medicaid. DIRM is remediating with DPH business oversight and participation.
- Health Plans that provide or pay the cost of medical care (e.g., Medicaid, Medicare, TriCare, BC/BS, HMOs). Government funded programs whose primary business is not providing for or paying the cost of medical care are excluded as covered health plans (e.g., Ryan White Sickle Cell, and Cancer Control Programs).
- Health care clearinghouses - not applicable to DPH

DEFINITION: PRIVACY

- Privacy is the right of an individual to keep his/her individual health information from being used or disclosed inappropriately for non-health related purposes.

- Privacy protections apply to Individually Identifiable Health Information (IIHI).

Definitions: PHI and IIHI

- PHI (Protected Health Information) - All **I**ndividually **I**dentifiable **H**ealth **I**nformation and other information on treatment and care that is transmitted or maintained in any form or medium (electronic, paper, oral, etc…)

- IIHI - any information, including demographic information collected from an individual, that:
  - Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and that
  - Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment of the provision of health care to an individuals; and that
  - Identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. These identifiers are listed on the next page.

Other HIPAA KEY TERMS Defined

- Use - means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
- Disclosure - Release or divulgence of information by an entity to persons or organizations outside of that entity.
- Authorization - The mechanism for obtaining consent from a patient for the use and disclosure of health information for a purpose that is not treatment, payment, or health care operations or not for other permitted disclosures such as those required by law and for public health purposes
- Minimum Necessary - When using any PHI, a covered entity must make all reasonable efforts to limit itself to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request”

HIPAA Privacy Regulation

- Regulates uses and disclosures of health information
- Establishes requirements to assure privacy of health information
- Sets appropriate safeguards to protect health information
- Ensures individuals have more control over when and how their health information is used
- Establishes new rights for individuals regarding access to their health information
- Strikes a balance between privacy of health information and protecting public health (e.g., reporting and tracking communicable diseases)

HIPAA Privacy Regulation

Individual Rights:

- Right to be informed by their treatment provider and health plans about protections on and use of their health information through a notice of privacy practices
- Right to inspect, copy, and review their records
- Right to request amendments to their records
- Right to request restrictions on use and disclosure of health information

HIPAA Privacy Regulation

Individual Rights:

- Right to request reasonable personal communications
- Right to an accounting of disclosures of their health information
- Right to file a complaint against covered entity

Also requires that covered entities refrain from requiring clients to waive their privacy rights as condition for treatment, payment, enrollment in health plan, or eligibility for benefits.

HIPAA Privacy Regulation

- HIPAA establishes a new federal floor of safeguards to protect the confidentiality of health information
- Preemption of state law
  - Privacy Rule overrides any other state law **unless** that state law provides more protection for the consumer (e.g., substance abuse and mental health statutes)

HIPAA Privacy Regulation

PRIVACY REGULATIONS RELATING TO
RESEARCH, MARKETING, FUND RAISING

- For research, marketing, and fund-raising purposes, health information must be de-identified (all individual identifiers must be removed)

- HIPAA still allows research to be conducted using individual health information:
  - With proper authorizations from individuals to use their health information
  - With an alteration to or waiver of authorization approved by an Institutional Review Board (IRB) that is established in accordance to federal law.

HIPAA Enforcement

- HIPAA carries significant civil penalties for failure to comply
- There are also criminal penalties for
  - Knowingly or wrongfully disclosing or health information protected by HIPAA
  - Committing offense under false pretenses
  - Intent to sell health information or client lists for personal gain or malicious harm
- HIPAA requires NC DHHS to establish personnel sanctions for employees who violate client privacy protections

HIPAA Enforcement

- **Centers for Medicare and Medicaid Services** is the designated enforcement agency for the HIPAA Transactions, Code Sets, Identifiers, and Security Standards.
- **US HHS Office for Civil Rights (OCR)** is the designated enforcement agency for the HIPAA Privacy Regulations. OCR will provide guidance and monitor compliance.
- **US Department of Justice (DOJ)** will be involved in criminal privacy violations. This agency will issue fines, penalties, and imprisonment.

Privacy in DHHS

- DHHS is a "hybrid entity." Its primary purpose is not to provide health care, but it has components that perform covered functions (health plans, health care services).
- The areas within DHHS that perform HIPAA-covered functions are called covered health care components. Health care components must comply with HIPAA.
- Business associates of health care components - A business associate performs functions specified by HIPAA on behalf of a covered entity (or health care component) that involves access to or exchange of health information.
  - Examples include claims processing or billing, accounting, consulting, legal, data analysis, data processing, quality assurance, utilization review.
  - Covered entities must gain formal assurances from their associates that they will provide privacy protection for health information. Business associates also must comply with HIPAA privacy regulations.

Privacy in DPH

- Within DHHS, DPH has covered health care components, including the State Laboratory for Public Health (indirect treatment provider) and the CDSAs.

- Within DHHS, DPH performs functions on behalf of covered health care components; for example, The State Center for Health Statistics provides data analysis, analysis for DMA and Medicaid Reimbursement, and Liaison provides cost analysis for DMA.

- DPH also performs functions on behalf of external covered entities; for example, Medicaid billing services via HSIS for local health departments and technical assistance for local health departments.

Privacy in DPH

- Privacy Regulation impact on CDSAs:
  - CDSAs are exempt from HIPAA Privacy Rule because their records are considered “education records” under FERPA (Family Educational Rights and Privacy Act).
  - CDSAs will follow and comply with FERPA privacy requirements and will also follow and comply with appropriate DHHS/DPH HIPAA compliant privacy policies and procedures.

Privacy in DPH

- Privacy Regulation impact on State Lab:
  - Follow and comply with appropriate DHHS/DPH privacy policies and procedures that apply to the Lab as an indirect treatment provider.
- Privacy Regulation impact on business associates within DPH:
  - Follow and comply with appropriate DHHS/DPH HIPAA compliant privacy policies and procedures.
  - Follow requirements for use and disclosure of health information formally defined by the covered health care component for whom the DPH business associate is performing services.

Privacy in DPH

- Privacy Regulation impact on DPH Program Areas:
  - Most DPH Programs are not health plans as defined by HIPAA.
  - DPH Program Participants, such as local health departments and public and other health care providers, however, are covered entities in their own right if they electronically process any of the defined transactions. They must also comply with HIPAA, and the impact of HIPAA on them is different than on DPH at the state level.
  - DPH Program Areas will follow and comply with appropriate HIPAA compliant DHHS/DPH privacy policies and procedures and give assurances to our partners that we are protecting health information.

Privacy in DPH

- All Medical Records in DPH are confidential per state public health law. These confidentiality protections extend beyond HIPAA covered components within DPH.
- § 130A-12. Confidentiality of records and § 130A-143. Confidentiality of records.
- All DPH staff must protect the confidentiality of medical information within DPH.

Privacy in DPH

- Release or disclosure of confidential information can only be made for purposes required by or allowed under state or federal law, for public health purposes, and for approved research.

- NC public health law aligns with HIPAA Privacy Regulation for the purposes of treatment, payment, research, or health care operations to the extent that disclosure is permitted under 45 Code of Federal Regulations §§ 164.506 and 164.512(i), which are sections of the HIPAA Privacy Regulation.

Privacy in DPH

- There is a risk that health care providers may resist providing health information to DPH, citing HIPAA.
- Public Health Exemption
  - HIPPA permits disclosures of IIHI without authorization for health information required by law (e.g., NC statue or administrative code) and allows for reporting for functions such as Vital Records.
  - HIPAA permits disclosures of IIHI without authorization to “public health authorities” for public health activities and purposes.
  - HIPAA permits disclosures of IIHI without authorization to a health oversight agency for oversight activities.
  - HIPAA permits but does not require public health disclosures.

Privacy in DPH

Public Health Exemption Guidelines

- Be knowledgeable about your program's/function's legal basis for collecting individually identifiable health information
- Restrict requests for health information to that which is required by law or to that which is minimally necessary to accomplish purpose
- Remember that public health data is still protected and its use is for public health purposes
- Know that there are other protections in addition to HIPAA govern health information:
  - Federal Laws
  - NC General Statutes
  - NC Administrative Codes
  - Professional Standards.

What HIPAA Requires of Everyone in DPH

HIPAA Requires DPH to…..

- Establish policies and procedures to protect and safeguard health information
- Develop disciplinary procedures for employees who intentionally violate privacy protection policies
- Define minimum necessary requirements
- Appoint a Privacy Officer
- Define a procedure to file and investigate complaints about violations of privacy protections
- Develop procedures for obtaining client authorizations to release their health information, where required
- Provide HIPAA training to the workforce, as necessary and appropriate, on Privacy Policies and Procedures.

Privacy Policies and Procedures

- **DHHS and DPH privacy policies to protect and safeguard PHI apply to all areas and employees within DPH** who create, maintain, or receive, use, or have access to individually identifiable health information during their regular course of business.

  All employees must ensure that individually identifiable health information is protected.

- Other specific HIPAA requirements and DHHS/DPH privacy policies and procedures apply only to certain areas within DPH, e.g., the State Lab, which is an indirect treatment provider. Information about these specific requirements is provided in additional material for those who need to receive the specific training.

Privacy Policies and Procedures

- DHHS privacy policies and procedures are documented in the DHHS Policies and Procedures manual, which are available on the DHHS website at

  DHHS Security & Privacy Policies
- NC DHHS is responsible for ensuring compliance by the agencies within NC DHHS.

Privacy Policies and Procedures

- DPH privacy policies and procedures are being documented in the DPH Privacy Policy and Procedures manual, which is available on the DPH HIPAA Privacy website at *NC DPH HIPAA Privacy Information*

- DPH has established an email address for you to ask questions and get answers about specific privacy and other HIPAA-related questions:

  HIPAA.DPH@ncmail.net

DPH Confidentiality Statement

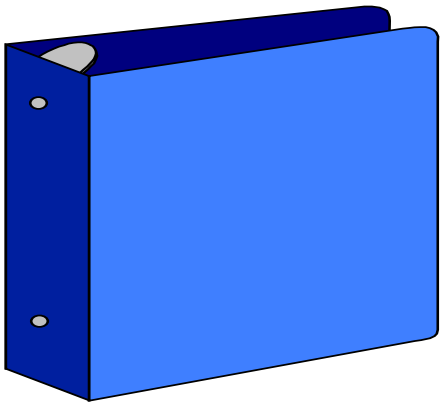
- **Employee Confidentiality Statement**
  - All DPH employees and extended workforce (e.g., contractors) must sign confidentiality statements:
    - Employees agree to protect the confidentiality of any individually identifiable health information to which they have access either directly or indirectly.
    - Employees must follow all NC DHHS and DPH business procedures to minimize the intentional or unintentional disclosure of individually identifiable health information to unauthorized parties.
    - Employees will take all reasonable efforts to limit individually identifiable health information to that which is necessary to accomplish the intended purpose, use, disclosure, or request for information.
  - You will sign this form after reviewing this training presentation.

Employee Sanctions

- **Disciplinary Actions**
  - Intentional violation of the terms of the confidentiality statement and inappropriate access/use/disclosure of IIHI can result in disciplinary action.
  - DPH will follow State Personnel procedures and work with NC DHHS Human Resources regarding any potential disciplinary actions.

Reminder - What is PHI ?

Protected Health Information - *All Individually Identifiable Health Information and other information on treatment and care that is transmitted or maintained in any form or medium (electronic, paper, oral, etc…)*



Challenge for DPH

- If you do NOT know *what* or *where* PHI is,
- and *who* uses or asks for it,
- You will be hard pressed to protect it.

Where do we find IIHI?

- Medical records and billing records
- Claims and payment information
- Program eligibility information
- Case or medical management records
- Program reporting from providers

IIHI exists both on paper and electronically and in oral communications

Reminder: PHI and IIHI Defined

- PHI (Protected Health Information) - All **I**ndividually **I**dentifiable **H**ealth **I**nformation and other information on treatment and care that is transmitted or maintained in any form or medium (electronic, paper, oral, etc…)

- IIHI - any information, including demographic information collected from an individual, that:
  - Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and that
  - Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment of the provision of health care to an individuals; and that
  - Identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. These identifiers are listed on the next page.

Individual Identifiers

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code…….
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death……..
- Telephone numbers
- Fax numbers
- Electronic 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…..

Any other unique identifying number or characteristic…..

How Individual Staff Protect IIHI

- Do not leave any records containing IIHI where others can see them or access them.
- Keep medical test results and all other medical information private.
- Do not share IIHI in public areas.
- Do not leave copies of IHI at copy machines, printers, or fax machines. Pickup printouts immediately.
- Verify and double check fax numbers before sending, and verify receipt of fax wherever possible.
- Do not leave IIHI exposed in mail boxes or conference rooms.
- Do not share computer passwords or leave them visible.
- Do not leave computer files open when leaving unlocked or shared work areas.
- Secure IHI when no one is in the area, either in locked file cabinets or locked in your office.
- Always safeguard IIHI when records are in your possession.
- Return all records containing IIHI to their appropriate location when you no longer require them.

How Individual Staff Protect PHI

Do Not:

- Email confidential and sensitive information with IIHI using unsecured email systems.
- Leave IIHI in any public wall file trays unless enclosed in an interoffice envelope.
- Discuss topics involving IIHI in front of other employees or visitors except on a “need to know” basis.
- Leave diskette boxes or Rolodex files containing IHI accessible in unlocked areas.
- Leave IIHI for shredding in unlocked/undesignated area.
- Leave records opened and unattended.
- Copy IIHI to your “personal” computer for use outside of authorized work areas.
- Leave door, cabinet, or card keys unattended.
- Delay in reporting lost or stolen keys.
- Share combination lock codes.

Uses and Disclosures

- **DPH must identify and document IHI Uses and disclosures**
  - WHO:
    - People who routinely use or disclose (or receive requests to disclose) PHI in our Division
  - WHAT:
    - Individually identifiable health information
  - HOW:
    - Written, oral, electronic communication
  - HOW MUCH:
    - Minimum necessary to accomplish purpose

Uses and Disclosures

- Before disclosing IIHI, we must verify the
  - Identity of person requesting the information
  - Authority of requestor to have access to the PHI
  - Specific information requested and specific purpose for the information

“Need to Know” Principles

- Necessary for your job
- How much do you need to know?
- How much do other people need to know?
- The key is to balance the privacy of health information against the need for information.

How Does “Need to Know” Translate into HIPAA?

- HIPAA’s Minimum Necessary rules :
  - Requires identification of employees who need access to PHI and the types (categories) of information to which access is needed
  - Staff must provide PHI only
    - in the minimum necessary amount
    - to accomplish the purpose for which use or disclosure is sought
  - Minimum necessary does not apply when patient provides a valid, signed authorization for release of PHI.
  - Verification is required from any person or organization requesting PHI, and you must determine or receive assurances that the request is for the minimum amount of information necessary to accomplish the purpose of the disclosure.
- *Exceptions:*
  - *Disclosure to a health care provider for treatment*
  - *Authorized uses or disclosures made by the patient.*
  - *Uses or disclosures made based on patient’s signed authorization*
  - *Use for legal proceedings, law enforcement, etc.*

How Does “Need to Know” Translate into DPH?

- DPH has developed a Minimum Necessary policy/procedure:
  - Managers in all DPH areas will identify the types (categories) of information in their areas and the employees who need access to that information to perform their jobs.
  - Managers will approve access to PHI based on a worker’s need to know.
  - Managers in all DPH areas will identify the information their area that is disclosed on a routine and recurring basis and document the purpose for the disclosure (e.g., required by law, public health reporting, etc.).
  - Managers will authorize which routine and recurring disclosures will occur, by which staff members, and under what conditions.

How Does “Need to Know” Translate into DPH?

- DPH has developed a Minimum Necessary policy/procedure:
  - Managers will review all non-routine disclosure requests on a case-by-case basis and ensure that information is not disclosed without the appropriate managerial approval.
  - Access and restrictions on information in computer applications will be restricted to the extent technically feasible based on an employee’s documented and approved need to know.
  - Disclosure of entire medical records is restricted to limited documented situations where access to the entire medical record is essential.

How Does “Need to Know” Translate into DPH?

- When
  - **Using** Protected Health Information
  - **Disclosing** Protected Health Information
  - **Requesting** Protected Health Information

  Make reasonable efforts to limit IHI to “minimum necessary” to accomplish the purpose.

- Do not disclose more than is necessary.
- Can you de-identify the information and still accomplish the purpose?
- Never send the entire medical record unless absolutely necessary!

DPH HIPAA Privacy Official

DPH has appointed Larry Forrister as Privacy Official as required by HIPAA:

- Serves as primary agency contact for privacy issues and concerns regarding the use and disclosure of health information and for appropriate client access to health information
- Serves as the DPH liaison to the DHHS Privacy Officer for privacy-related activities
- Coordinates and facilitates DPH's efforts to accomplish its privacy compliance
- Acts as the DPH point of contact for all privacy-related questions:

HIPAA.DPH@ncmail.net

DPH HIPAA Privacy Complaints

- **DPH Complaint Procedure**
  - Allows a consumer, including you as an employee, to file a complaint if they believe DPH has improperly used or disclosed their PHI
  - All complaints and their resolution are documented
  - To file complaints:

    - DPH Privacy Office via email at HIPAA.DPH@ncmail.net

    or by mail at

    - DPH Privacy Official
      1931 Mail Service Center, Raleigh, NC 27699-1931

REFRAIN FROM INTIMIDATING OR RETALITORY ACTS

HIPAA protects individuals who exercise their privacy rights and also protects whistleblowers. Covered entities, including DHHS/DPH, may not:

- Intimidate
- Threaten
- Coerce
- Discriminate against
- Take any other retaliatory action against

employees for exercising their privacy rights under HIPAA, including their right to file complaints.

Authorizations

- **Authorization by Client**
  - Is required to disclose IIHI to a person or agency outside the Division, with permitted exceptions
  - Must be specific
    - What IIHI is to be shared
    - With whom
    - For what purpose
  - May be revoked by client
  - Must be obtained on HIPAA-compliant standard DPH Authorization form, which will available on the DPH website.

Authorizations

- **Authorizations Requested from DPH**
  - Must be reviewed to ensure that request is a valid authorization that complies with HIPAA requirements
  - Must be approved by designated DPH manager before information is released

When No Authorization Is Needed…

- Key examples:
  - Disclosure is required by law
  - Disclosure is for public health purposes
  - When required for program monitoring and evaluation
  - To avert serious threat to health or safety
  - Child abuse/neglect reports.

QUESTIONS?

If you are ever in doubt about anything related to HIPAA and DPH privacy, **always** ask your Privacy Officer or their designee!

HIPAA.DPH@ncmail.net

Key Things to Remember about Privacy

- We must vigorously safeguard all client-protected health information.
- We should use and share only the client information necessary to do the work.
- Clients have the right to ask about use and disclosure of PHI.
- DHHS and DPH has policies on HIPAA, and you need to know them and follow them.

Privacy vs. Security

- Privacy is the right of an individual to keep his/her individual health information from being disclosed.

- Security is how we protect PHI from accidental or intentional disclosure, alteration, destruction, or loss.

Purpose of Security

- To protect the system and information from unauthorized access
- To protect the system and information from unauthorized use

General Security Awareness

- Security (protecting the system and the information it contains) includes

  protecting against unauthorized access from outside and misuse from within.

General Security Awareness

- Guidelines for workplace security
  - Follow all building and work area security procedures.
  - Display proper identification.
  - Identify yourself when asked.
  - Be aware of visitors in your work area. If they can't be identified, ask why they are there - politely ask if you can be of assistance.
  - Secure work areas when leaving for the day.

PC and System Protection

- Do not share any computer session unless your job specifically requires it.
- Follow the NC DHHS computer use policy.
- Do not download or install non-DPH approved programs.
- Report unknown or suspicious email and email attachments.
- Ensure that a DPH-authorized screen saver is installed with password protection.
- Log out of the applications and/or the system when you leave or walk away from your computer.

Password Management

- What is Password Protection?
  - Do not tell anyone your password.
  - Do write your password down or post it anywhere.
  - Change your password regularly.

Password Management

- Guidelines for good passwords
  - **Do Not**
    - Choose a password that can be found in a dictionary
    - Choose passwords that uses information about you, such as SSN, credit card, or ATM #, birthday
    - Use password that others can connect to you, e.g. , name of spouse, children, pets, favorite sports team, etc.
    - Use a password that uses your user id or any variation.
    - Reuse old passwords or any variation of them.

Where To Go For More Information

- DPH Privacy Office email at HIPAA.DPH@ncmail.net

  DPH HIPAA Privacy Information

  NC DPH HIPAA Privacy Information
- NC DHHS HIPAA Web Site NC DHHS HIPAA
- NC DHHS Privacy & Security Policies

  ND DHHS Security & Privacy Policies
- US Department of Health and Human Services

  Health Care Administrative Simplification
- Center for Medicare and Medical Aid Services

  http://www.cms.hhs.gov/HIPAAGenInfo
- Office of Civil Rights

  HHS - Office for Civil Rights - HIPAA
- CDC HIPAA Information

  Privacy Rule Facts
- UNC School of Government

  UNC School of Government: HIPAA and Medical Confidentiality

Document(s) Signature Required

Each employee is required to sign the following two documents.

Please print each document separately, sign and return as noted.

Training Record

Please print this form and complete the required information to acknowledge that you have received this training material and reviewed for understanding of compliance requirements. Make a copy for your records and return the completed form to:

DPH Human Resources/HIPAA Coordinator

1930 Mail Service Center

Raleigh, NC 27699-1930.

Training: "NC DPH Privacy Basic Training"

Date Completed: _____

Print Name: _____

Signature: _____

Section: _____

DPH Confidentiality Statement

Please also sign the DPH Confidentiality Statement located at:

http://www.schs.state.nc.us/hipaa/policies/DPHPriv-203B-Confidentiality-Agreement.doc

Make a copy for your records and return the completed form along with your signed Training Record to:

DPH Human Resources/HIPAA Coordinator,

1930 Mail Service Center. Raleigh, NC 27699-1930.