Division of Public Health Required Privacy Training

Reviewed and Updated
March 29, 2018

Federal Privacy Protections

- The right to informational privacy under the Fifth and Fourteenth Amendments to the Constitution;
- Federal assurance of confidentiality under section 308(d) of the Public Health Service Act; and,
- The federal Health Insurance Portability and Accountability Act (HIPAA) of 1996

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 providing healthcare treatment:

  SLPH is an Indirect Treatment Provider

- Healthcare providers who conduct any of the HIPAA-regulated transactions electronically:

  The SLPH submits claims electronically to Medicaid.

Who is Covered by HIPAA?

- DHHS is the organization that is a covered entity under HIPAA
- It is a “hybrid” entity that contains both covered and non-covered components
- The SLPH is a covered healthcare component within the NC DHHS hybrid covered entity.

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)

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.

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 all medical information.

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.

  SLPH posted on website

- Right to inspect, copy, and review their records.

  Recent CLIA amendment to allow

- Right to request amendments to their records – NA.
- Right to request restrictions on use and disclosure of health information – NA.

HIPAA Privacy Regulation

Individual Rights:

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

See next page

- 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.

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.

Requirements for the confidentiality and security of confidential data

Purpose

- Provide reasonable and appropriate safeguards for securing confidential and sensitive information
- Provides written uniform standards and procedures to protect against confidentiality breaches
- Provides written documentation that supports our intention to safeguard confidential information

Guiding Principles

1. PHI will be maintained in a physically secure environment.
2. Electronic PHI data will be held in a technically secure environment, with access limited to a minimum
3. All staff is responsible for protecting confidential surveillance information and data.

Guiding Principles cont.

4. Breaches of confidential surveillance information or data will be investigated thoroughly, and sanctions imposed as appropriate.
5. Security practices and written policies will be continuously reviewed, assessed and as necessary, changed to improve the protection of confidential surveillance data.

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.

Definitions: PHI and IIHI

- IIHI - any information, including demographic information collected from an individual, 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.
- PHI (**P**rotected **H**ealth **I**nformation) - 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…).

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…..

De-Identification

- § 164.514 Other requirements relating to uses and disclosures of protected health information.

- (a) *Standard: De-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

De-Identification

(b) *Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(i) Applying such principles and methods, 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 a subject of the information;

See Handout

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”

“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.

Data Collection & Use

Access to Confidential Patient Data

- Authorized staff are those whose job duties require access to public health records, laboratory reports, medical records, etc.
- This authorization must be based on a public health need.

Data Collection & Use

- Access to information or data for non-public health purposes, such as litigation, discovery, or court order, must be granted only to the extent required by law.

- Verify any requests for access to surveillance have been approved by the proper authority.

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

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

  protecting against unauthorized access from outside and misuse from within.

How Individual Staff Protect PHI

- Do not leave any records containing PHI where others can see them or access them.
- Keep all other medical information private.
- Do not share PHI in public areas.
- Do not leave copies of PHI 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 PHI 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 PHI when no one is in the area, either in locked file cabinets or locked in your office.
- Always safeguard PHI when records are in your possession.
- Return all records containing PHI to their appropriate location when you no longer require them.

How Individual Staff Protect PHI

Do Not:

- Email confidential and sensitive information with PHI using unsecured email systems.
- Leave PHI in any public wall file trays unless enclosed in an interoffice envelope.
- Discuss topics involving PHI in front of other employees or visitors except on a "need to know" basis.
- Leave diskette boxes or Rolodex files containing PHI accessible in unlocked areas.
- Leave PHI for shredding in unlocked/undesignated area.
- Leave records opened and unattended.
- Copy PHI 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.

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.

Safeguards Summary

- Handout
- Available at

  http://publichealth.nc.gov/employees/dphit/securityTraining/SafeguardsSummaryGuidelines2014-May.pdf

- Post in your work areas

Physical Security

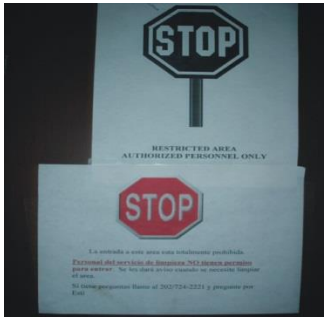
- Work areas
- Computer workstations
- File storage
- Courier and regular mail
- Interoffice mail
- Fax
- Disposal of confidential information

Physical Security

- Every employee is Responsible for Protecting their work area.
- All staff is responsible for reporting suspected security breaches.

Physical Security

- All documents containing patient identifiers must be stored in locking file cabinets or desks.
- All *PHI must* be stored securely.



Physical Security

- Access to any secured areas that either contain PHI by unauthorized individuals can only be granted during times when authorized staff are available for escort or under conditions where the data is secured.

- Unauthorized staff shall not be permitted into secure work areas without approval of the supervisor in charge of the area. Staff are responsible for ensuring that all other staff are aware of any visitors to secure areas so precautions can be taken to secure confidential data

Physical Security - FAX Transmissions

- Should be sent and received within the secured area, if the fax contains confidential information.
- Use a cover page containing a statement about confidentiality.
- Should not link personal identifiers and disease related information whenever possible.

Physical Security - *FAX Transmissions*

- Always confirm the recipient's fax number.
- When faxing to a new source, ask or confirm if the recipient's fax machine is located in a secured location.

Oral Communications

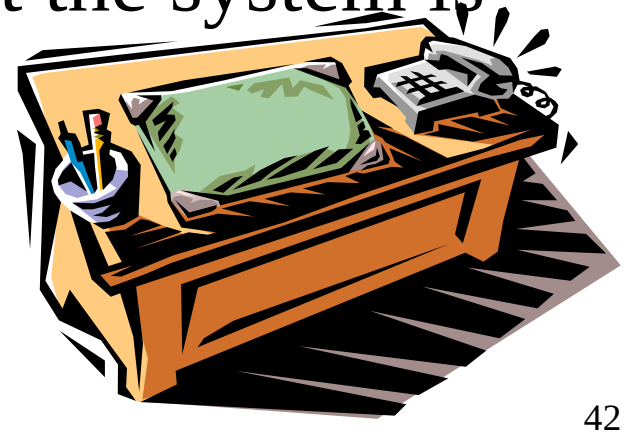
- Oral conversations
  - In-person
  - telephone

Physical Security - Speaking

- Confidential or sensitive information should NEVER be discussed outside of the restricted access area if there is any chance that it may be overheard.

Phone Messages

- Messages linking patient identifiers and disease information should not be left on any voicemail system unless you have determined in advance that the system is confidential.



Disposal

- Staff must shred documents containing confidential information before disposing of them. Shredders should be of commercial quality with a crosscutting feature.

Mail

- Regular and courier mail
  - Follow the procedures for your office
  - Double envelop confidential information
    - Inner and outer envelopes should be properly labeled and directed to a person with an address
    - Mark the inner envelope confidential
    - Avoid disease identifying information on the outer envelope

Interoffice

Double envelop confidential information

- Inner and outer envelopes should properly labeled and directed to a person with an address
- Mark the inner envelope confidential
- Avoid disease identifying information on the outer envelope

Removal Prohibited

- SLPH data, particularly PHI, must not be taken to private residences unless specific documented permission is received from authorized staff.

Electronic Security

- Email
- Data transfers
- Data in transit
- Data storage – efiles
- Laptops and removable storage devises

Electronic Security

All staff must be individually responsible for protecting their own workstation, laptop, or other devices. This responsibility includes protecting keys, passwords, and codes that would allow access to confidential information or data.

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.

Electronic Security - *Communication*
Email

- Internal or external email shall not be used to transmit sensitive or confidential information unless it has been properly encrypted.

  Bottom line for staff:

  Do not email confidential information.

  Remember

  There is no such thing as a TOTALLY secure fax or email transmission.

Electronic Security

- Any electronic devices removed from secure work areas with confidential information must be encrypted according to Departmental (DHHS) standards.

DPH 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.

Employee Sanctions

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

Why Comply?

- 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!

HIPAA Enforcement

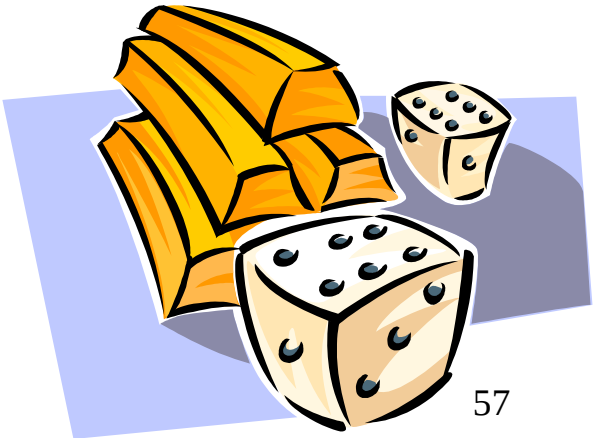
- HIPAA carries significant civil penalties for failure to comply
- There are also criminal penalties for
  - Knowingly or wrongfully disclosing or health information protected by HIPAA
  - Committing offense under false pretenses
  - Intent to sell health information or client lists for personal gain 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.

DO NOT RISK IT!

- Studies show that 80% of sensitive data losses come from lost laptops or employees ignoring security policies.



QUESTIONS?

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

or (me)!

HIPAA.DPH@ncmail.net

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 Privacy & Security Policies**

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

  Health Care Administrative Simplification
- **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

?? Questions ??