Keep It Confidential!

Georgia’s HIV Program

Security and Confidentiality Training

Audience: HIV Prevention & CARE Staff / Presenter: Ebony Wardlaw, MPH
Date: November 30, 2018
Agenda

- HIPAA
- CDC/HRSA Expectations
- Security
  - Physical Security
  - Electronic Data Security
- Email Communication
- Breach of Confidentiality
Objectives

- Understand your role protecting client specific HIV data

- Understand the basic principles behind patient confidentiality and why it is important

- Understand the components of H.I.P.A.A. and other regulations, as well as HIV-specific policies surrounding patient confidentiality, privacy and security
2018 Breaches

As of August 2018, over 200 health data breaches affecting over 6 MILLION individuals

2018 security vulnerabilities

- Hacking or IT incidents
- Unauthorized access or disclosure breaches
- Theft or loss
- Improper disposal
- Unencrypted computing devices
2018 Breaches

January 2018 - Aetna Agrees To Pay $17 Million In HIV Privacy Breach

- 12,000 insured receiving mailings that disclosed HIV drug info through clear window of the envelope
- 13,500 names released to Aetna’s legal counsel and a vendor without proper authorization

2018 Breaches

March 2018 Federal Lawsuit Filed Following Alleged CVS Health Data Breach

- Ohio Department of Health contracted with CVS to provide HIV medications through ADAP

- Mailings exposed PHI of over 6,000 individuals, including HIV status

July 2018 - Tennessee Health data breach exposes information on thousands of HIV patients

- Personal health information (PHI) of thousands of HIV/AIDS patients from Enhanced HIV/AIDS Reporting System (eHARS) database in Nashville

- Data should only been available to THREE employees but was left accessible on shared computer server that 500 employees throughout agency could access

- Also included SS numbers, lab results, other details (sexual orientation/illegal drug use)

Security, Confidentiality & Privacy

- A major concern

- Secure and confidential collection, storage, usage, and transmission of sensitive HIV/AIDS information is KEY

- Not protecting health information is AGAINST THE LAW
What is HIPAA?
Health Insurance Portability and Accountability Act of 1996

ANN, I’M NOT SURE THAT’S WHAT HIPAA HAD IN MIND
What is HIPAA?
Health Insurance Portability and Accountability Act of 1996

- 1996 Health Privacy Legislation fully enacted in April 2005
- Limits how we use and share patient information
- Gives patients more control over their information
- Protects the integrity, availability and confidentiality of patient information
- Defines violation penalties
- Penalties, including fines of up to $250,000 and 10+ years of imprisonment
What is Protected under HIPAA?

- Identifiable health information created or received by a health care provider, employer, or plan.

- In any form: written, verbal, electronic

- Information on HIV, alcohol and drug treatment, psychotherapy notes, etc. has even more stringent protections.
In Addition to HIPAA...

More Federal Regulations

*At the national level, HIV information is protected by a Federal Assurance of Confidentiality under Section 308(d) of the Public Health Service Act, 42 U.S.C. 242m(d), that prohibits disclosure of identifiable information that could be used to directly and indirectly identify individuals.

In Addition to HIPAA...

Georgia Regulations

- The HIV/AIDS Program is authorized under Georgia Surveillance Law (O.C.G.A. §31-12-1) to conduct notifiable disease surveillance of HIV and AIDS

- Public health activities are not subject to HIPPA restrictions

- Health Care Providers must complete a case report form within 7 days on newly diagnosed patients, new patients in their care, and patients with changes in disease status

- Laboratories must report all HIV indicative lab results
In Addition to HIPAA...

- Georgia Department of Public Health Information Security Policy (7/2018)

- Higher level policy where most expectations are the same as what is required in HIV-specific regulations
Paragraph 807 under Computer and Communications Systems Usage states:

Electronic mail must not be used to communicate confidential information unless ...it is encrypted.
What Does All This Legal Stuff Mean?

In addition to *possible termination*, *criminal charges* can be pressed against individuals, including state or local public health employees, who disclose information inappropriately.
GA HIV Program’s Security, Confidentiality & Privacy Training

- Annual training for all HIV staff

- All employees, including contractors and volunteers, are required to sign the state’s HIV confidentiality agreement
CDC/HRSA Expectations

As a condition of funding

• The CDC requires all federally funded Viral Hepatitis/HIV/STD/TB Surveillance programs (Funding Opportunity Announcement PS18-1801) to have a security and confidentiality policy.

• HRSA requires a security and confidentiality policy that includes control systems to ensure safeguards of protected personally identifiable information

• Local entities should discuss data security protocols with internal HIPAA privacy officer/IT Security staff/Security Officer
Building Trust: Confidentiality and the Ryan White HIV/AIDS Program

Impact of security and confidentiality in treatment of clients and on data collection within HIV programs

Available at: https://hab.hrsa.gov/livinghistory/issues/Confidentiality.pdf
- Released in 2011
- Establishes S&C standards for HIV, STD, TB, and Viral Hepatitis programs
- Available at: http://www.cdc.gov/nchhstp/programintegration/docs/pcsidatasecurityguidelines.pdf
CDC’s Ten Guiding Principles

1. Public health data should be acquired, used, disclosed and stored for legitimate public health purposes.

2. Programs should collect the minimum amount of personally identifiable information (PII) necessary to conduct public health activities.

3. Programs should have strong policies to protect the privacy and security of PII.

4. Data collection and use policies should reflect respect for the rights of individuals/community groups and minimize undue burden.
Ten Guiding Principles, Cont’d

5. Programs should have policies and procedures to ensure the quality of any data they collect or use.

6. Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.

7. Programs should share data for legitimate public health and may establish data-use agreements to facilitate sharing data in a timely manner.
Ten Guiding Principles, Cont’d

8. Public health data should be maintained in a secure environment and transmitted through secure methods.

9. The number of persons and entities granted access to identifiable data should be minimized.

10. Program officials should be active and responsible stewards of public health data.
Definitions

- Confidentiality
- Security
- Privacy
- Personally Identifiable Information (PII)
- Breach of Confidentiality
Confidentiality

The right of an individual to have personal, identifiable medical information kept private.
Security

Protection of public health data and information systems to prevent unauthorized release of identifying information and accidental loss of data or damage to the systems.

Security measures include measures to detect, document, and counter threats to data confidentiality or the integrity of data systems.
Privacy

Practice of maintaining the security and confidentiality of patient records, involving both the conversational discretion of health care providers and the security of medical records.
Personally Identifiable Information (PII) or Personal Health Information (PHI)

- Any information that would enable a person’s identity to be established
  - *Direct identifiers* – e.g., name, social security number or other information that is unique to an individual
  - *Indirect identifiers* – e.g., uncommon race, ethnicity, extreme age, unusual occupation and other details, especially in combination with each other or other information
Breach of Confidentiality

An unintentional/intentional release or disclosure of personally identifiable information to unauthorized persons (e.g. employees or members of the general public)
Potential Sources of Risk

- Viewing, transmitting or moving identifiable information (electronically, hard copies, fax, cell camera phones)
- Access to secure area
- Communications (verbal, electronic, written, email, telephones)
- Lack of training and/or lack of agreements
Security

- Physical Security
  - Personally identifiable program data must be maintained in a physically secure environment, such as a restricted access area with locking file cabinets

- Electronic Data Security
  - Identifiable electronic data must be held in a secure environment, with the number of individuals permitted access kept to minimum
Physical Security and Data Movement

To the extent possible, ensure that persons working with hard copies of documents containing confidential, identifiable information do so in a secure, locked area.

Minimum Secure Area:
- Work space with limited access for only necessary staff
- Locked file cabinets that are large and heavy enough to render them immobile
- A designated location within the work space where confidential conversations may be held
Destroying Paper Documents

- Corporate shredding services who can ensure confidential shredding
- Manual shredding by Agency staff
Destroying Paper Documents

*Ensure that documents containing confidential information are shredded with crosscutting shredders before disposal*

- Crosscutting features are needed to ensure confidential information cannot be recovered.
- If a commercial shredding service is used, they must be bonded, and due diligence should be taken in the selection of the company.
Record Retention

Ensure that data-security policies and procedures address records and data retention

- How long should you keep Viral Hepatitis/HIV/STD/TB-related test/medical information?
- Record retention policies vary by agency- Know Yours!
- If electronic copies exist, paper copies can be destroyed when no longer needed, in accordance with established policies (if applicable).
Important!

- Paper copies of any protected health information can constitute a security risk if they are lost, misplaced or stolen.

- Avoid a HIPAA violation and destroy paper records per your local record retention policy!
Physical Security

- Rooms containing public health data should not be easily accessible by window

- If people can potentially see through windows, close blinds when using the computer

- Monitor screens provide an additional level of security
Simple physical theft is a major cause of health information breaches

- Only take needed data out of the office with Supervisor approval

- Protect line list and reports by transporting them in a locked briefcase and/or encrypted USB Drive
Simple physical theft is a major cause of health information breaches

- Ensure documents do not contain term “HIV” or related terms (e.g. CD4 counts, viral load)

- All documents containing PII must be returned to a secure environment by the close of business each day unless:
  - Prior approval has been received
  - Employee is in possession of appropriate means of securing the information as outlined above
Physical Security (Continued)

- Staff Responsibilities

  - Ensure security of individual workstations

  - Any loose paperwork containing sensitive information should be cleaned off desktop and locked securely in a drawer when you leave the office and at the end of every workday
Physical Security (Continued)

- Lock computer screen every time leaving the computer, even for a few minutes
- Wear employee identification badge
- Properly destroy documents containing confidential information per your program’s guidelines
Electronic Data Security

Four data systems used:

- **CAREWare**
  Part B Clinical Data/ADAP

- **eHARS**
  Surveillance

- **Evaluation Web**
  Counseling and Testing

- **SENDSS**
  Partner Services, Linkage, etc
Electronic Data Security

- Authentication
  - Ensuring identity of users is confirmed
- Data Integrity
  - Protecting data from unauthorized users
- Do NOT share passwords with anyone
- Do NOT sign on and allow someone else to access data
Electronic Data Security

- If fax machines are used, they should be maintained in a secure locked space

- Only use printers that do NOT store information on an internal hard drive

Do not leave sensitive information on the copier!!!
Digital Photocopiers and Data Security

Digital Photocopiers Loaded With Secrets

At a warehouse in New Jersey, 6,000 used copy machines sit ready to be sold. CBS News chief investigative correspondent Armen Keteyian reports almost every one of them holds a secret. Nearly every digital copier built since 2002 contains a hard drive - like the one on your personal computer - storing an image of every document copied, scanned, or emailed by the machine.

In the process, it's turned an office staple into a digital time-bomb packed with highly-personal or sensitive data.

If you're in the identity theft business it seems this would be a pot of gold.

"The type of information we see on these machines with the social security numbers, birth certificates, bank records, income tax forms," John Juntunen said, "that information would be very valuable."

Even the use of photocopy machines can put people at risk of having their personal information exposed.

Bottom Line: Organizations should ensure that all PII is protected, particularly in places where they are least suspected of being released.

Electronic Data Security (Continued)

- **Electronic Databases**
  - Electronic databases should be maintained on secure servers with backups performed regularly on secure servers
  - Only required staff should have access to databases with the minimum level of access granted to fulfill job responsibilities (i.e., read only access)
  - Once access is no longer required, user accounts should be deactivated as soon as possible
Electronic Data Security (Continued)

- Destruction of Data
  - Computer disks and hard drives are wiped prior to destruction
  - Hard drives of computers, scanners, and copy machines should be physically removed and destroyed
Email Communications

DO NOT:

- Send emails that contain PII including:
  - Patient names, DOB, SSN, Home Address, ANY PII, eHARS Unique Identifiers
- Send files over the internet without approval
- Place PII in subject line of an email (or anywhere else in the body of the email)
Access and Transmitting Electronic Info

- Staff may need to transmit:
  - Line lists
  - Maps
  - Claims information
  - Many other forms of identifying data

- DO:
  - Secure File Transfer Portal (SFTP)
  - Encrypted USB
Email Communications

**DO:**

- Always think carefully before hitting SEND: is there anything potentially identifiable in this email?
- When requesting information, make sure that it is clear to the recipient that they must not send identifying information back by email (don’t assume they know this)
Security, Confidentiality & Privacy

- All discussions pertaining to confidential information are conducted in secure private areas. Medical record reviews are conducted as discreetly as possible.

- Client information should never be shared with other healthcare providers without first having a **Release of Information** signed by the client.
Security, Confidentiality & Privacy

- **Mail**
  - **Outgoing**: Managed by the health department and U.S. federal mail. All confidential information is placed in double envelopes, with “Confidential” marked on the inner envelope. No envelope should have any direct or indirect reference to any disease.
  - **Incoming**: Only designated staff opens program mail and distributes to appropriate person.
Security, Confidentiality & Privacy

- Incoming Telephone Calls
  - Generic identifiers (e.g., “Department of Health, this is Name”), without direct reference to the particular disease(s) are used to answer all incoming calls

- Outgoing Telephone Calls
  - Staff should discuss confidential information so as not to be overheard by others, release information to only those individuals with a need-to-know, and always use utmost discretion
Cellular Phone Service

- Cellular phone transmission is NOT secure. Never use patient-identifying information during a cellular phone call. Callers should refer to specific individuals by state or some other reference that is familiar to the recipient of the information. If patient-identifying information must be shared, the caller should return the call from a landline telephone.

Laptops, PDAs, & Portable Storage Devices

Laptops and other portable devices (e.g., PDAs, tablet personal computers, floppies, thumb drives) that receive or store confidential information with personal identifiers must incorporate the use of encryption software.
Security Breaches

- All staff are responsible for reporting suspected security breaches to your immediate supervisor or the Overall Responsible Party (ORP)

- A breach of confidentiality must be immediately investigated to assess causes and implement remedies
Breach of Confidentiality

- Penalty for unauthorized release of information
  - Breach of security and confidentiality pertaining to confidential information may result in suspension, demotion or termination based on the severity of the offense
  - The severity of the offense and appropriate disciplinary action for HIV staff with access to data will be determined by local program management, the ORP, HR, and/or the Legal Affairs Office
Remember

- Security & Confidentiality is EVERYONE’S responsibility
- Exercise good judgment in the daily management of all public health information
- No manual or training can cover everything
- Ask your supervisor for guidance when an issue is unclear
Remember

- As public health workers, we have an obligation to conduct our jobs in a manner that protects the confidentiality of clients infected with HIV/STD/TB/hepatitis or other diseases, and to maintain the public trust.
- Destroy data if it is no longer needed.
- Secure and confidential collection, storage, use, and transmission of HIV information is central to programmatic success.
Remember

There is not a blue print for every situation!
Remember

- Being a responsible steward of public health data means to be aware of issues and threats to data security. In addition, asking the questions that are needed to protect data:
  - Is this the least amount of data needed to accomplish the task?
  - Does this person have authority to access?
  - Am I transporting this correctly?
WE CHECKED YOUR CONFIDENTIAL MEDICAL RECORDS ON THE INTERNET. CHEESE AND ANCHOVIES WOULD BE BAD FOR YOU, SO WE LEFT THEM OFF.
Who to Contact?

Ebony Wardlaw, Overall Responsible Party (ORP)
HIV Data Program Manager

ebony.wardlaw@dph.ga.gov

404-657-3127
Thank You!