
NC DPH: Computer Security Basic Awareness Training

Introduction and Training Objective

- Our roles in the Division of Public Health (DPH) require us to utilize our computer resources in a manner that protects public health interests.
- More specifically, federal and state privacy and security regulations mandate that we protect and safeguard the access, use, and disclosure of confidential information.
- Education and training is one aspect of ensuring we protect our clients' confidentiality.
- There are two phases of training all DPH information system users are required to complete.
  - The DPH Basic Privacy Training helped explain "what" information is considered confidential. You were required to take this training as part of your orientation when you joined DPH.
  - This second phase, DPH Basic Security Training, explains some basics of how to safeguard confidential health information as you use DPH information systems.

Training Instructions

- Review this presentation and follow the instructions on the last slide to indicate that you have completed the training.
- Review the “Acceptable Use for DHHS Information Systems” policy and sign the “User Certification of Notification of Agreement of Computer Use Policy” (as described in the next slide).

Acceptable Use for DHHS Information Systems

- All DPH employees and extended workforce (e.g., contractors) who have access to DPH computer systems and electronic data must:
  - Read the Acceptable Use for DHHS Information Systems Policy.
  - Acknowledge that they have done so by signing the User Certification of Notification and Agreement of Computer Use Policy.
  - Follow the measures described in the policy when using state information systems.
- All users must agree to use the state's computer systems responsibly to conduct government business according to the terms in the acceptable use policy.

The policy is posted with this training on the DPH website at http://www.ncpublichealth.com/dphit/dphit_security.htm.

HIPAA Privacy and Security Applicability

Federal Law:

HIPAA Privacy & Security Regulations mandate protection and safeguards for access, use, and disclosure of PHI and/or ePHI with sanctions for violations.

HIPAA applies to HIPAA Covered Health Care Components within the Division (e.g., SLPH).

Security of confidential information applies to all DPH business units and staff.

Privacy versus Security

- Privacy is the right of an individual to keep his/her individual health information from being used or disclosed other than for its intended purpose. It applies to Protected Health Information (PHI), which is individually identifiable health information in all its forms (e.g., paper records, reports, phone conversations, verbal consultations).
- Security applies to protected health information in electronic format and is how we protect electronic PHI (ePHI) from accidental or intentional misuse, disclosure, alteration, destruction, or loss.

Definition of “ePHI”

- ePHI or electronic Protected Health Information is patient health information which is computer-based (e.g., created, received, stored or maintained, processed and/or transmitted in electronic media).
- Electronic media includes computers, laptops, disks, memory sticks, PDAs, servers, networks, dial-modems, E-mail, Web sites, medical devices, medical test equipment, etc.

Computer Security Focuses on Confidential Electronic Information

- Examples of ePHI:
  - Medical record number, account number, SSN.
  - Patient demographic data (e.g., address, date of birth, date of death, gender, E-mail / web address).
  - Dates of service (e.g., date of tests or treatment).
  - Medical records, reports, test results.
- Other Confidential Information:
  - Employee personal information.
  - Security plans.

What is Computer Security for the Protection of ePHI?

Definitions:

Computer Security means ensuring the confidentiality, integrity, and availability of ePHI through safeguards. Safeguards protect computer systems and the electronic information within them against unauthorized access from outside the organization and from misuse from within the organization.

- **"Confidentiality"** – ensure that confidential information will not be disclosed to unauthorized individuals or organizations.
- **"Integrity"** – ensure that data or information has not been altered or destroyed in an unauthorized manner. Ensure that data from one system is consistently and accurately transferred to other systems.
- **"Availability"** – ensure that data or information is accessible and usable when needed by an authorized person.

ePHI Security Standards

- Ensure the confidentiality, integrity, and availability of the electronic protected health information (**ePHI**) that the entity creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI (e.g., hackers, viruses, data back-ups).
- Protect against unauthorized disclosures.
- Train workforce members ("awareness of good computing practices").
- Use and share only the client information necessary to accomplish specific work and for which authorization has been provided.
- Report anything unusual – notify your manager, the DPH Security Official, or DPH LAN Support if you become aware of a suspected computer-related security incident.

Why Comply with the Security Standards?

- Protecting client health information
  - Is required by law!
  - Is the right thing to do!
- Protecting the confidentiality of our clients' health information is critical to maintaining trust and confidence in the public health system.

What are the Consequences of Security Violations?

- Risk to integrity of confidential information (e.g., data corruption, destruction, unavailability of patient information for treatment).
- Risk to security of personal information (e.g., identity theft).
- Embarrassment, bad publicity, media coverage, news reports.
- Loss of client trust, employee trust and public trust.
- Internal disciplinary action, up to termination of employment.
- Penalties, prosecution, and potential for sanctions / lawsuits.

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.

How Individual Staff Protect Health Information

- Do not leave any records containing health information where others can see or access them.
- Keep medical test results and all other medical information private.
- Do not share health information in public areas.
- Do not leave copies of health information at copy machines, printers, or fax machines. Pick up printouts immediately.
- Verify and double-check fax numbers before sending, and verify receipt of fax wherever possible.
- Do not leave health information exposed in mail boxes or conference rooms.
- Do not leave computer files open when leaving unlocked or shared work areas.

How Individual Staff Protect Health Information

- Secure health information when no one is in the area, either in locked file cabinets or locked in your office.
- Always safeguard health information when records are in your possession, whether in the office, at home, or in transit. Lock the information in a safe location at home, the office, or in the car.
- Return all records containing health information to the appropriate location.
- Do not delay in reporting lost or stolen keys or badges.
- Do not share combination lock codes, keys, or badges.
- Do not allow anyone to “tailgate” behind you into restricted areas.
- Do not take home sensitive information without appropriate supervisor authorization.
- Do not discuss topics involving health information in front of other employees or visitors except on a “need to know” basis.

How Individual Staff Protect Health Information

- Do not E-mail confidential and sensitive information or ePHI using unsecured E-mail systems unless it is in password-protected files.
- Never send a password via E-mail.
- Do not copy confidential information to your “personal” computer for use outside of authorized work areas.
- Do not leave diskettes, CDs, or other portable storage media containing health information accessible in unlocked areas.
- Always sanitize media (CDs, disks, hard drives) before reusing them (contact DPH IT Support to sanitize media).
- Do not leave health information for shredding in unlocked/undesignated area.
- Secure your workstation when unattended, including using strong passwords, approved screensavers, logging off, and locking your session.
- Follow the Acceptable Use for DHHS Information Systems policy.

Password Management

- Protect your password:
  - Do not tell anyone your password.
  - Do not write your password down or post it anywhere.
  - Change your password regularly.
  - Use “strong” passwords.

Password Management

- Guidelines for strong passwords
  - **<u>Do:</u>**
    - Choose a password that is at least 8 characters long.
    - Use a combination of letters and numbers.
    - Include both upper and lowercase letters.
    - Include at least one special non-alphanumeric character (e.g., !@#$%^&*()+?).
    - Change your password regularly.

Password Management

- Guidelines for strong passwords
  - **Do Not:**
    - Choose a word that can be found in a dictionary.
    - Choose passwords with personal information (e.g., SSN, credit card #, ATM #, birthday, name of spouse, children, pets, favorite sports team, etc.).
    - Use a password that repeats your user id or any variation of it.
    - Reuse old passwords or any variation of them.

PC and System Protection

- Follow all security policies, procedures, and regulations regarding the use of state computer resources .
- Do not share any computer session unless your job specifically requires it.
- Do not download or install non-DPH approved programs.
- 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.
- Lock-up! – offices, windows, workstations, sensitive papers and PDAs, laptops, mobile devices / storage media.
  - Lock your workstation (Ctrl+Alt+Del <Enter> for Windows XP, Windows 2000
  - Maintain control of keys and badges.
- Report unknown or suspicious E-mails and E-mail attachments.

E-Mail Security – Risk Areas

- **Spamming.** Unsolicited bulk E-mail, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers.
  - Do not reply to spam messages. Do not spread spam. Remember, sending chain letters is against state policy.
  - Do not forward chain letters. It's the same as spamming!
  - Do not open or reply to suspicious E-mails. Delete the message.

- **Phishing Scams.** E-mail pretending to be from trusted names, such as Citibank or Amazon, but directing recipients to rogue sites. A reputable company will never ask you to send your password through E-mail.

- **Spyware.** Spyware is adware which can slow computer processing down, hijack web browsers, spy on key strokes, and cripple computers.

- Opening E-mail attachments that may contain malicious code, such as viruses. All users are responsible for helping to prevent the introduction and spread of computer viruses and other "malware."

Should You Open the E-mail Attachment?

- If it's suspicious, delete and don't open it!
- What is suspicious?
  - Not work-related.
  - Attachments not expected or from someone you do not know.
  - Attachments with a suspicious file extension (*.exe, *.vbs, *.bin, *.com, *.scr, *.pif).
  - Contains web links.
  - Unusual topic lines: “Your car?”, “Oh!” , “Nice Pic!”, “Family Update!”, “Very Funny!”.

Report Computer Security Incidents

- Report computer security incidents & breaches **immediately** to:
  - DPH IT Support at **919-707-5160.**
  - IT Support will coordinate response and inform the DPH Security Official.
- Users must notify LAN Support **immediately** if they know or suspect that their network account or workstation has been compromised by a virus or unauthorized access.
- Other types of reportable computer security incidents are listed on the following slide.

Computer Security Incidents

- **Computer Security Incident –** A violation (or imminent threat of a violation) of computer security policies, acceptable use policies, or standard computer security practices. A Computer Security Incident is an adverse event where a North Carolina information system is accessed or used without authorization; attacked or threatened with attack; or used in a manner inconsistent with established policy with the potential to cause the real or possible loss of confidentiality, integrity, or availability of the resource or its information.
- Some examples of computer security incidents include:
  - Unauthorized attempts (either failed or successful) to gain access to a state-owned/operated/managed system or its data.
  - Unauthorized or misuse of a system for the processing or storage of data.
  - Intentional or unintentional disruption of processing capability or denial of service (DoS) attacks.
  - Actual or suspected loss of confidential, proprietary, or entrusted information.
  - Using information systems to commit financial crimes or cause financial loss to the State or the citizens of North Carolina.
  - Changes to system hardware, firmware, or software configurations without appropriate approval.
  - Malicious software (virus, worm, Trojan horse) attacks.
  - Attempted or actual instances of social engineering (e.g., phishing scams).
  - Perpetration of hoaxes.
  - Copyright violations.
  - Unauthorized network scans or probes.

System Activity Review

- Monitoring of Use
  - Any activity conducted using the State's information systems, including E-mail and the use of the internet, may be logged, monitored, archived or filtered, either randomly or systematically.
  - All network accounts and workstation hard drives are subject to periodic audit for the purpose of maintaining security and license requirements.
  - Both DHHS and the Division reserve the right to perform these actions without specific notice to the user.

Employee Sanctions

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

QUESTIONS?

If you are ever in doubt about anything related to HIPAA and DPH security (or privacy), **always** ask your supervisor or the DPH Security and Privacy Official!

HIPAA.DPH@dhhs.nc.gov

919 715-0411

DPH Information Security Official

DPH has appointed Larry Forrister as Security and Privacy Official as required by HIPAA and NC DHHS Policy:

- Serves as primary agency contact for computer security privacy issues and concerns regarding the protection and safeguarding of Electronic Protected Health Information.
- Serves as the DPH liaison to the DHHS Security Office for computer security-related activities.
- Coordinates and facilitates DPH's efforts to accomplish its security compliance.
- Acts as the DPH point of contact for all computer security-related questions:

  HIPAA.DPH@dhhs.nc.gov

  (919) 715-0411

Documents Signature Required

- Each employee, contractor, et al., is required to sign the following two documents:
  - Training Record (next slide).
  - “User Certification of Notification and Agreement to Acceptable Computer Use” (included as part of the “Acceptable Use for DHHS Information Systems” policy, which must be reviewed as part of the Basic Security Training).
- Please print each document separately, sign, and return as noted.

DPH Computer Security Basic Awareness Training Record

Please print this form (in black and white) 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 Basic Computer Security Awareness Training"

Date Completed: _____

Print Name: _____

Signature: _____

Section: _____