Information Privacy and Security Training 2018

Authored by:
Office of HIPAA Administration
Objectives

After you finish this Computer-Based Learning (CBL) module, you should be able to:

- Define privacy practices and Protected Health Information (PHI).
- Explain the basic concepts of information security.
- Explain your security responsibilities and the part you play in protecting sensitive information and assets belonging to GHS.
Topics Covered in this CBL

- What needs to be protected?
- What is Protected Health Information?
- What is Information Security?
- What are the consequences of Privacy or Security failures?
- What are the types of Security failure?
- How can we safeguard patient information from accidental or malicious use or disclosure?
What is HIPAA?

- HIPAA stands for the Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

- This law provides for both the privacy protection and security of electronic medical records.
Basic HIPAA Rights for the Patient

- Every patient has basic HIPAA rights.
- These are communicated to our patients in the Notice of Privacy Practices posted in our registration areas and on our website, and as a copy offered to the patient at the time of registration.
Protected Health Information

- **Protected Health Information** (PHI) is health or medical information linked to a specific individual’s:
  - Identity – demographic and financial data, or
  - Medical condition and treatment – clinical data.

- PHI is individually identifiable information created, maintained or received by a:
  - Healthcare provider,
  - Health plan, or
  - Healthcare clearinghouse.

- PHI relates to the past, present or future:
  - Physical or mental health condition of individual, or
  - Payment for the provision of health care to an individual.
Examples of Protected Health Information

- Name
- Address
- Age
- Social Security Number
- Phone number
- Email address
- Full Face Pictures
- Medical record number
- Diagnosis
- Medical history
- Medications
- Observations of health
- And more....
What Needs to be Protected?

- **Protected Health Information (PHI)** is protected under the Privacy Rule and is defined as all “individually identifiable health information” whether electronic, paper or oral.

- **Electronic PHI (ePHI)** is PHI stored on or transmitted by computer, mobile device or network, including:
  - USB drives
  - Cell phones
  - iPads
  - CDs
  - Smart phones
  - Computer files
  - Clinical equipment
**Privacy and PHI**

**Minimum Necessary**

- “**Minimum Necessary Information**” means the only information the receiving party has a legitimate clinical and/or business **need** to know.

- Be sure you disclose, fax, copy, and print **only** the minimum necessary patient information for the purpose.

- The GHS Minimum Necessary policy states that associates are **not allowed** to access their own, a relative’s, a friend’s, or anyone else’s medical record if they are not involved in the individual’s medical care.
Privacy and PHI

Transmission of PHI

When emailing, copying, printing, faxing, or scanning:

- Do not leave copies unattended on shared equipment.
- Always email from a GHS email address, for example:
  - “...@gwnnettmedicalcenter.org”.
  - ”...@gwinnetttmedicalgroup.com”.
- Verify the destination information to be sure you are sending the information to the correct location.
- If your email is being emailed to an email address other than @gwinnettmedicalcenter.org then you need to put [secure] in the subject line to encrypt your email.
- For example: **Subject:** [secure] Stuff About Patient
Privacy and PHI

Transmission of PHI

When faxing, use the GHS-approved fax cover sheet with confidential health information and warning.

- You can find the approved fax cover sheet at GMCConnect/Quick Links/Forms/Click on the letter “F” in the upper center of the screen.

“Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either.”
Cost of Misdirected Faxing

Two misdirected faxes cost a hospital $387,200 in a HIPAA settlement.

1. One fax went to patient’s employer in error.
2. Another fax went to unintended recipient.
Privacy and PHI

Communication

To protect a patient’s privacy:

- If the patient’s friends or family are in the room, do not discuss PHI without the patient’s permission; ask.
- Avoid using patients’ names in public hallways and elevators.
- Know who the patient has designated as his or her personal representative before discussing PHI.
- Especially remember to protect highly sensitive PHI: HIV, STDs, and Mental conditions.
Privacy and PHI

GHS Is Committed to Privacy

- Let our patients know that GHS values and protects their privacy.
- Tell patients when you are taking privacy precautions.
  - For example: say, “To protect your privacy, I am...”
    - “Speaking in a low voice.”
    - “Asking visitors to step out of your room.”
    - “Pulling the privacy curtain.”
Privacy and PHI

Privacy Policies

You can access the privacy policies covered in this CBL on GMCConnect by clicking on “Policies” and then selecting the “HIPAA Privacy” System Manual.
Privacy and PHI

Other Important Reminders

- Disposal of printed material
  - The only proper method of disposing of paperwork containing sensitive patient information is to shred it.

- Patient medical records
  - Never leave a medical record out and open.
  - Never leave a medical record unattended in a patient’s room.
  - If a medical record is not in use or is going to be unattended, place it face down or in its appropriate storage location.

- “No Information” patients
  - Never confirm or acknowledge a “no information” patient is at a GHS facility; for example, say “I have no information on a patient of that name.”
What is Information Security?

**Information Security** is the process of ensuring the confidentiality, integrity, and availability of information through appropriate safeguards.

- **Confidentiality:**
  - Prevents unauthorized access or release of PHI.
  - Prevents abuse of access, such as identity theft, gossip.

- **Integrity:**
  - Prevents unauthorized deletion or changes to PHI.

- **Availability:**
  - Prevents service disruption due to malicious activities, accidental actions, or natural disasters.
What is Information Security?

Regulations and Standards

GHS Information Security policies and procedures are based on the following regulations and standards:

• Health Insurance Portability and Accountability Act (HIPAA)
• National Institute of Standards and Technology (NIST) standards
• Health Information Technology for Economic and Clinical Health (HITECH) Act
• Payment Card Industry (PCI) standards
• Joint Commission (JC) accreditation
What is Information Security?

Information Security Policies

You can access the Information Security policies covered in this CBL on GMCConnect by clicking on “Policies” and then selecting the “HIPAA Security” System Manual.
Information Security Mascot

- KIP is the GMC mascot for the HIPAA Privacy and Security Training and Awareness program.
- KIP is short for “Keep Information Protected”.
- You can email KIP at: KIP@gwinnetttmedicalcenter.org
Types of Security Failure

There are two types of security failure:

1. Intentional attack, and...
2. Workforce member carelessness.

1. **Intentional Attack**
   - Malicious software (viruses)
   - Stolen passwords
   - Impostors calling or e-mailing to steal information (phishing)
   - Theft (laptop, smart phone)
   - Abuse of privilege (employee/VIP clinical data)
   - Social engineering (talking someone into giving access that is not authorized)
Types of Security Failure, continued

2. Workforce Member Carelessness

- Giving a patient/family documents from another patient’s records.
- Sharing passwords
- Not signing off of computer systems
- Downloading and launching unauthorized software
- Improper use of e-mail and web surfing
- Not questioning or reporting suspicious or improper behavior
- Negligence
Consequences of Security Failure

Security failure can result in:

- Disruption of patient care.
- Increased cost to the organization.
- Legal liability and lawsuits.
- Negative publicity.
- Identity theft (monetary loss).
- Disciplinary action.
- Loss of public confidence.
Protection Against Security Failures

You can protect against security failure by:

- Creating “strong” passwords.
- Using e-mail and the internet appropriately.
- Securing desktops and portable devices.
- Disclosing only the “minimum necessary” PHI.
- Reporting breaches.
Create Strong Passwords

- **Do** choose strong passwords. A strong password:
  - Is at least 8 characters long, and ...
  - Contains a combination of capital letters, lower case letters, numbers, **and** special characters.
- **Don’t** share your passwords.
  - **You** are responsible for the actions of others when they use your computer or user and password credentials.
- **Don’t** store passwords in your office or where they are accessible to others.
- **Don’t** use the “remember password” feature on computer systems.
- **Do** change your password if you suspect a breach, and report it to the CRC at x23333.
Protecting Against Security Failures

Appropriate Use of E-mail, Internet

- When you use GHS information technology and computer systems, your activities are not private.
- GHS monitors activity that occurs on its network, including:
  - Access to patient information
  - Internet use,
  - Corporate e-mail,
  - Web-based e-mail (Yahoo, Hotmail, Gmail), and
  - Instant messaging.
Protecting Against Security Failures

Appropriate Use of E-mail, Internet

- GHS monitors computer use to ensure that:
  - Sensitive information is sent out correctly.
  - No harassing or pornographic communications are taking place.
  - Associates are using time and resources appropriately.
  - Associates are not viewing inappropriate websites.
- If you misuse GHS computer equipment or internet access, you are subject to disciplinary action.
Protecting Against Security Failures

Appropriate Use of E-mail

- Do not open e-mails from someone that you do not know.
- Do not forward work e-mails to a non-GHS e-mail account.
- Do not send e-mails that contain:
  - Profanity, obscenities or derogatory remarks.
  - Pornographic material.
  - Threats and hate literature.
  - Chain letters inside or outside the organization.
  - Sexual, ethnic, racial, or other workplace harassment.
Appropriate Use of E-mail

- Be aware of risks, including spam and phishing e-mails.
  - Spam is unsolicited bulk e-mail, including:
    - Commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers.
    - Do not reply to or forward spam messages.
  - Phishing e-mails pretend to be from trusted names, such as Citibank, PayPal, Amazon, even co-workers, but give you directions to malicious sites.
    - Never click on a link in a suspicious e-mail.
    - A reputable company will never ask you to send your password through e-mail.
- Forward spam and phishing e-mails to KIP@gwinnetttmedicalcenter.org.
Protecting Against Security Failures

Appropriate Use of the Internet

- You may not visit inappropriate Internet sites or engage in inappropriate communications.
- Examples of sites or communications that are inappropriate include:
  - Pornographic
  - Culturally offensive
  - Racist or hate-related
  - Related to gambling
  - Related to computer hacking
  - Terroristic
Computer viruses are dangerous programs that:
- Run on a computer without the knowledge or permission of the user, and ...
- Are meant to damage your computer or to gain access to your information.

Viruses can:
- Spread onto computer discs and across a network.
- Corrupt data files.
- Format or erase your hard drive.
- Delete files.
- Install software that will allow a hacker access to your system.
- Send sensitive information to unauthorized parties.
Protecting Against Security Failures

Secure Desktops and Mobile Devices

- Log off and exit computer programs when leaving a work station.
- Ensure that your computer screen is turned so that passersby cannot read information on the screen.
- Use an encrypted USB drive if you must store or transport data.
  - Do so only if there is a business purpose.
  - Contact the CRC at x23333 to obtain an encrypted USB drive.
Secure Desktops and Mobile Devices

Notebook computers and mobile devices:

- **Never** leave them unattended.
  - Lock them up!
- **Never** leave them visible in your car.
- Store as little sensitive information on them as possible.
- If your notebook computer or mobile device is lost or stolen, report it to the CRC x23333 and Public Safety department **immediately**.
Protecting Against Security Failures

Social Engineering

Be aware of **social engineering**, which is the process of tricking or manipulating someone into giving access to sensitive information. Examples include:

- **Tailgating**: One or more person(s) follow(s) an authorized person through a secured door or other entrance.
- **Shoulder surfing**: Direct observation techniques, such as looking over someone’s shoulder to get information.
Protecting Against Security Failures

Social Engineering

- **Impersonation**: A person pretends to be someone they are not in order to gain information.
  - For example, you receive a phone call from someone claiming to be a PC tech or GHS associate requesting such information as:
    - Passwords,
    - User name, or
    - Other sensitive information.
Protecting Against Security Failures

Media Disposal

- You must dispose of media (disks, paper, etc.) containing sensitive information so that the information cannot be accessed by any unauthorized person.

- Proper media disposal methods include:
  - Paper records: place in shred bins.
  - CDs, film, discs, and other media:
    - Lawrenceville: Take to Information Services Operations.
    - Duluth: Take to media disposal bin by the loading dock.
  - Hard disc drives: Contact the CRC at x23333.

- Just erasing data does not actually remove it!
Protecting Against Security Failures

Social Networking

- Get approval from your manager before accessing social networks using GHS devices or systems.
- Do not use information gained as a result of your position with GHS to contact or communicate with:
  - Patients,
  - Clients, or
  - Third-party business associates.
- Do not post any GHS-related information on social media like FaceBook, Twitter, LinkedIn, SnapChat etc.
- Do not share information related to:
  - Our corporation,
  - Patients, or
  - Clients.
Protecting Against Security Failures

Social Networking

• Represent GHS in a professional manner at all times.

• If you post anything from a GHS e-mail address:
  • Include a disclaimer stating that the opinions you’ve expressed are strictly your own and not necessarily those of GHS.
  • Exception: The posting is in the course of business duties and has been approved by the GHS Marketing and Communications department.
Privacy and Security Breaches

“Breach” means the unauthorized acquisition, access, use, or disclosure of PHI.

- Someone sees information they’re not allowed to see.

- Breach fines and penalties can be brought against **an individual**, not just GHS.

- In some cases, a breach must be reported to:
  - The patient,
  - The media,
  - The Office for Civil Rights/Department of Health and Human Services.
Breaches

Civil Monetary Penalties Law

- Breach fines and penalties can range into the **millions** of dollars.
- The government may seek civil monetary penalties for a wide variety of fraudulent and abusive conduct in addition to:
  - Exclusion from the Medicare and Medicaid program,
  - Criminal conviction, and
  - Jail time.
Breaches

Report Incidents or Breaches

If you believe an Information Security incident or a breach has occurred:

- Let your manager know.
- Report incidents or breaches of sensitive GHS information to:
  - www.gwinnettmemorymedicalcenter.ethicspoint.com or,
  - Call the Corporate Compliance Hotline: 888-696-9881.
Breaches

Report Incidents or Breaches

When you report an incident or breach, the Office of HIPAA Administration will:

- Investigate,
- Perform risk analysis/mitigation of harm,
- Notify patient, if necessary, and
- Notify regulatory agency, if necessary.
Breaches

Report Incidents or Breaches

GHS takes disciplinary actions in response to confirmed information breaches.

- If you fail to report a known or suspected breach, or if you report a breach for malicious reasons, you might receive a disciplinary action.
- Office of HIPAA Compliance investigates all suspected Privacy and Information Security breaches.
- Disciplinary action may result in termination of employment.
- All confirmed allegations of breach are subject to risk assessment and disclosure to the U.S. government Health and Human Services Department.
- GHS can take no retaliatory action against any workforce member who in good faith makes a report, complaint or inquiry.
Congratulations!

- You have completed this CBL module.
- Continue on to complete the Information Privacy and Security Acknowledgment.
- Questions? Contact HIPAA Administration:
  - Compliance Manager/Information Privacy and Security: 678-312-4243
  - Privacy and Security Coordinator: 678-312-3793
  - Compliance Hotline: 1-888-696-9881