Federal: Privacy and Security

Topics

- What are privacy and security all about?
- What's confidential here?
- How can I protect confidential information?
- What should I do if I see a problem?
- How can I get more information?

What are privacy and security all about?

What is privacy?

- Information privacy
  - is about a person's control over their personal information
  - and the responsibilities of organizations that have personal data.
- We care about everyone's privacy, but we need to take special care with patient (or plan member) information.

What is HIPAA?

- “HIPAA” – federal law giving patients certain privacy rights, such as:
  - Look at and receive a copy of their own medical and billing records
  - Request an amendment to these records
  - Request limits with respect to how their information is used and released
- HIPAA also requires healthcare organizations and their business associates to do the following:
  - Follow rules pertaining to use and release of patient information
  - Keep patient information private and confidential, safe and accurate
- (For Covered Entities) HIPAA privacy rights and organization commitments are described in our “Notice of Privacy Practices.” Know what’s in our Policy and where to obtain a copy.

What is security?

- Information security provides three important qualities:
  1. ***Confidentiality*** – No one has access to the information absent authorization and a work-related need. For example, payroll access is only for payroll staff. (Managers may have some access to their own staffs' payroll records.)
  2. ***Integrity*** – The information can be trusted and hasn't been changed or deleted by accident or through tampering. For example, laboratory results can be critical for patient treatment.
  3. ***Availability*** – Information is there when needed for work. For example, emergency department access to medical records (paper or electronic) is important for care.

The connection between privacy and security

- Privacy and security are connected. We need security, especially confidentiality, to ensure that patient information is kept private

Why am I reading and hearing this?

- HIPAA requires healthcare organization and their business associates to teach employees, staff, volunteers, students and residents about privacy and security so that patient privacy is protected.
- Following good privacy and security practices is also good sense. It protects all important information at this organization.
- This describes some key policies and what is expected of you. Each person is responsible for following these privacy and security policies and practices. Everyone's commitment is needed to maintain privacy and security in this organization.

What’s confidential here?

What is “confidential” here?

- Remember, “confidential” means people who need the information for work can get it, but others can’t.
- The organization’s policies protect confidential information including:
  - Patient information
  - Some employee information – such as a person’s Social Security number and salary
  - Certain business documents – such as business plans, legal cases and others
- Confidential information can be in any form: oral, paper and electronic. It’s in patient and personnel records, and also conversations, telephone message slips, email, faxes, laptop computers and thumb drives, just about everywhere!

Confidential patient information

- Healthcare organizations have always treated a patient’s medical information, such as diagnosis and test results, as confidential.
- But now HIPAA defines confidential patient information as everything about a patient – including name, address, medical record number and other demographic and billing information – as well as all of the patient’s medical information.
- Any information that could identify a specific patient is confidential, even if the patient’s name is omitted. For example, a patient with a rare condition could be identified simply by that condition and perhaps, the month of admission or date of visit.
- HIPAA calls this Protected Health Information or **PHI**.

HIPAA and common sense
(for healthcare provider organizations)

- HIPAA permits certain disclosures of PHI without written permission:
  - Family and friends: If a patient is with a family member or friend, physician (or other staff) should ask if a private conversation is preferable. Use professional judgment, but make it comfortable for the patient to say "private."
  - Facility directory: Unless a patient opts not to be listed in the directory, anyone who asks for a patient by name can be told the patient's general condition and location. Clergy members may have lists of patients (who have not opted out) by religious affiliation.

HIPAA and common sense (cont’d)

- Sign-in sheets and whiteboards:
  - Use minimum information on sign-in sheets (e.g., patient name and appointment time). Keep whiteboards out of patients’/visitors’ sight if possible; if not, show the least necessary information.
- Unavoidable (“incidental”) disclosures are not violations if reasonable steps are taken. Examples: One patient recognizes another in a waiting room; an inpatient overhears her roommate’s discussion with her physician.
- Most importantly, never discuss patients for social reasons; keep it strictly business. Be cautious, but HIPAA should never interfere with patient care.

How can I protect confidential information?

Where are the dangers?

- Natural and environmental: Fire, earthquakes, power outages and burst water pipes damage confidential paper records and computer systems. Systems may crash or become victim of a computer virus, potentially damaging information and causing systems to be unavailable when needed.
- The BIGGEST threats come from **people**, both insiders and outsides.
  - Accidents, carelessness or curiosity lead to inappropriate conversation about patients, unauthorized record access, failure to shred paper or sending a confidential fax to the wrong number.
  - Deliberate actions such as using someone else’s ID and password without their knowledge, maliciously changing or deleting data, or copying data such as patient credit card detail for identity theft.

Practical steps for keeping information confidential and safe

- Lower your voice or conduct confidential conversations in a private place. Don’t speak with/about patients in an elevator unless no one else is present.
- Don’t leave patient records unattended in areas where patients/visitors are present. Don’t leave confidential paper on copiers, printers fax machines.
- Always shred paper containing confidential information, including patient information (even name and telephone number) before discarding. Shred fax machine ribbons and carbons also.
- When faxing confidential information, always use a cover sheet with a confidentiality notice, double check the recipient’s fax numbers and follow all procedures.

More practical steps for keeping information confidential and safe

- Check your computer screen angle. If visible to the public, adjust it or use a filter. This applies to all devices, including mobile.
- When leaving your work area, store confidential materials and log off, lock or shut down your computer.
- Be aware of strangers who may not belong in a secure area (e.g., records file room, server room, laboratory).
- Keep locked doors locked. If you need to use a swipe care to enter a secured area, close the door behind you. Don’t allow tailgating.

Exercise special care when releasing patient information

- Follow procedures, especially when releasing information to an outsider. Be careful about giving information about a patient to the following individuals:
  - Someone working here
  - Family and visitors
  - Some other third party
- Follow special procedures when PHI is used for research
- Ensure that you know what to do. Follow the “minimum necessary” rule without compromising patient care.
- If it’s not your job to provide information, ask a manager or refer the requester to the Privacy Officer.

Just because you can…

- Don’t abuse your access privileges. Just because you can do something doesn’t mean you’re authorized or permitted to do it.
- In a file room or database, access only specific records when you have a work related need. Example: Patient care staff may access their patients’ paper and electronic medical records, but they’re not permitted to access other patients records, even with good intentions.
- Administrator or super-user privileges: Only use powers as required by your job. Examples: Super-users may be able to create user accounts, but only when and as authorized. Email administrators may monitor when cause, but not permitted to browse email for non-work purposes.

Select good passwords and keep them secret

- Good passwords are easy for you to remember and difficult for someone else to guess!
- Make up your own secret method. Select a theme, then key phrases and initial letters. Your password will appear meaningless, but you'll be able to remember it.
- Don't share your password with anyone…. Would you share your toothbrush? And don't write it anywhere it could be found and used. Change it whenever you think someone else knows it.
- Follow standards for password length, content and frequency of change. Be sure to use a mix of numbers, upper- and lower-case letters and special characters.
- Don't use the same password everywhere, and especially don't use the same password for home personal use and at work.

Using computers and our network

- Follow policies and use only for legitimate business purposes. Incidental personal use is permitted if it doesn’t interfere with job performance, affect or degrade system resources and particular use is not prohibited.
- Unless required by your job, don’t install software (apps) or hardware on organization devices/network; don’t create Web pages, electronic bulletin boards or other public access to our network/resources.
- Computing resources may not be used for personal or financial gain. Any activity that puts our organization at risk is prohibited unless it is a documented part of the job.
- Note: Network and systems may be monitored.

Portable computers and media

- Portables include laptops, tablets, PDAs, smart phones, CDs, flash or thumb drives and even some MP3 players.
- Since these items are portable, they are easy to lose. They’re also high-theft items. If lost or stolen, confidential data or access to our network could be compromised.
- So if you use portable equipment, especially outside the facility, you must take great care.
- Don’t leave these items unattended in your care, meeting rooms, public transportation, hotels, or elsewhere. Lock them up and put them out of sight. Use cable locks or lock items inside cases.
- Any device or electronic medium that may be used to access or store confidential information must use encryption.

Portable device setup

- Portable devices must be set up to do the following:
  - To require you to enter your secret password to use the device
  - To lock or log off automatically after a period of inactivity (but this is only a safety net…. be sure to lock or log off)
  - With a firewall, and with anti-virus/anti-malware installed, updated and run automatically
  - So that the operating system, browser and other software are kept current with security updates
  - Without any file sharing application
  - With remote disable or “wipe” capability enable
  - With encryption to protect any saved data. This applies to portable media also. Protect your encryption key and keep it secret (never save it on the device or medium). Consult IT for any questions.

Working off-site

- If authorized and required for your job, you may work off-site, and you may need to access our network from your home or on the road. Like working with portable devices and media, working offsite carries some special risks, so it's important to follow policy.
- Don't copy and remove confidential information unless it is required by your job and has been authorized. Transport it securely in a locked container. Shred paper and adequately delete files when no longer needed. (Remember that clicking "delete" does not actually delete a file or folder.)
- Transmission of confidential information over public networks including the Internet and wireless networks requires encryption. Ask for help from IT if you have questions.

Using the Internet “cloud” safely

- Cloud services are convenient, but they can be risky. This is particularly true of free services such as email and word processing apps and storage. (Also, they may require that a Business Associate contract be signed.) There may be better alternatives. Always discuss with your IT consultant/ department first.
- Be very careful when downloading apps for a device such as a portable computer or smartphone. Many apps contain malware that can steal your password or our confidential information and more. First, consult IT, or research the app through reputable sources.

Transmitting confidential information

- All transmission of confidential information via the Internet, another organization's network and wireless networks (even at home) must be encrypted.
    - You may have been given access to our network through an encrypted VPN (virtual private network)
    - You may access a secure website (HTTPS) for applications and email
    - If you connect from a wireless network at home, it must be configured securely
- Because text messages are not secure, texting of our confidential information, including images, is prohibited.
- Ask IT if you have questions. Always ask before transmitting information in a new way.

Using social networks

- Social networks can be fun, creative ways to interact with people locally and around the world. But their openness means that nothing you say is private.
- Before you log on to Facebook, Twitter, Blogspot or any other social networking site, remember not to discuss your work, our patients or this organization without first reading and following our policy and guidelines for acceptable use of social networking sites.
- Never discuss a patient in any way that could be used to identify the person. Remember that patients (or their families) might identify themselves even if no name or other direct identifiers are used.

Using email safely

- Don’t use personal email accounts (e.g., Hotmail, Gmail) for business and don’t forward confidential business email to you home account.
- Email confidential information such as PHI with care. If the message is leaving our network, it must be encrypted.
- Be cautious about opening suspicious email and attachments because they may contain computer viruses and other malicious software. Also beware of “phishing” emails that ask you to click on a link, taking you to a legitimate-looking, but fraudulent, banking or other business website where you are asked for personal information such as a bank account number, Social Security number, password or PIN. Legitimate organizations will not contact you this way.
- Do not use instant messaging or “chat” for business purposes.

What should I do if I see a privacy problem?

Mandatory incident reporting

- You must promptly report any suspected or actual violation or breach of our privacy and security policies to your Privacy Officer.
- This includes attempted or successful unauthorized access, use, disclosure, modification or destruction of our information. It includes intrusion and interference with our computer systems
- This also includes policy violations, even if you are unsure whether the violation led to a breach. Examples include failure to log off or to shred confidential papers.
- This organization must be able to respond whenever there is a privacy or security problem. But we may not know about it unless you report it.

Examples of incidents you should report

- Medical records are found in an unprotected area where they shouldn’t be
- Patient-identifiable information is found in the trash
- A laptop computer, possibly containing confidential information, is stolen
- A staff member looks up a patient in a computer system when he or she shouldn’t
- A computer is left logged on and unattended
- A fax with confidential information is sent to the wrong number
- An email with patient information is sent to a group of individuals when only one person should receive it
- A thumb drive with patient information is lost
- A computer is infected with a virus

Look for suspicious signs when you log on and use your computer

- When you log on, check the message telling when you last logged on (if your system displays this information). If it says you were logged on when you don't think you were, report this as an incident. Someone may be using your ID and password.
- When you log on, if there are changes in the way your screen looks or new software appears unexpectedly, report it. While logged on, if your computer is persistently much slower than usual, report it. These could be signs of malicious software ("malware").

Sanctions

- A violation of our policies can lead to a breach that has negative consequences for the individual and the organization.
- Therefore, when a member of our workforce is involved in a privacy or security incident, we are required by HIPAA and best practices to consider disciplinary action and further steps if appropriate.
- Our disciplinary actions will be based on the severity of the incident, intent and pattern of behavior, along with fairness and consistency.
- HIPAA requires us also to consider notifying professional credentialing bodies if appropriate, law enforcement agencies and the US Department of Health and Human Services. Violations of HIPAA regulations can lead to federal, civil and criminal penalties including fines and imprisonment.