Valley Regional Medical Center
HIPAA AND HITECH EDUCATION

Privacy and Security of Protected Health Information

HIPAA and Its Purpose

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- Federal law in response by Congress for healthcare reform
- Mandatory, civil and criminal penalties for failure to comply

Purpose

- Protect health insurance coverage, improve access to healthcare
- Reduce fraud and abuse
- Improve quality of healthcare in general
- Reduce healthcare administrative costs (electronic transactions)
- Affects all healthcare industry

HITECH and Its Purpose

What is HITECH?

- Health Information Technology for Economic and Clinical Health Act
- Subtitle D of the American Recovery and Reinvestment Act of 2009 (ARRA)
- It’s a federal law

Purpose

- Makes massive changes to privacy and security laws
- Applies to covered entities and business associates
- Creates a nationwide electronic health record
- Increases penalties for privacy and security violations

Key HITECH Changes

- Breach Notification requirements
- AOD for treatment, payment, and healthcare operations in electronic health record (EHR) environment
- Business Associate Agreements
- Restrictions
- Right to access
- Criminal provisions
- Penalties
- OCR Privacy Audits
- Copy charges for providing copies from EHR
- HIPAA preemption applies to new provisions
- Private cause of action
- Sharing of civil monetary penalties with harmed individuals

Protected Health Information (PHI)

- Relates to past, present or future physical or mental condition of an individual; provisions of healthcare to an individual; or for payment of care provided to an individual.
- Transmitted or maintained in any form (electronic, paper or oral representation).
- Identifies the individual or can be used to identify the individual.

Examples of PHI

Health information may be considered individually identifiable if any of the following are present:

- Name
- Address including street, city, county, zip code and equivalent geocodes
- Names of relatives
- Name of employers
- Birth date
- Telephone numbers
- Fax Numbers
- Electronic e-mail addresses
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic, code

PHI Considerations

- **Use Caution with Communication Processes**
  - ✓ Do not leave patient voicemail messages regarding procedures, or diagnosis codes.
  - ✓ DO NOT DISCUSS PHI with unauthorized individuals. Never tell a friend, family member or co-worker who you have seen or treated at the facility.
  - ✓ Bragging to individuals not involved in a patient’s care is a direct violation of the law.
  - ✓ Always give your patient the opportunity to object to having healthcare discussed in front of family/visitors.
  - ✓ Do not leave PHI (billing or clinical) on your desk, printers, copiers, or fax machines – this includes claim forms and fax transmission confirmations!
  - ✓ Never leave electronic health record unattended in patient care areas.
  - ✓ Pulling privacy curtains and lowering voices as appropriate.
  - ✓ Abbreviated patient names on white boards and outside of the patient rooms.

PHI Considerations (cont.)

- **Use Caution with Documentation**
  - ✓ Do NOT dispose of any medication packaging that contains patient information in regular trash.
  - ✓ When faxing PHI, know (verify) the receiver, use pre-programmed numbers when possible and approved fax cover sheets when faxing outside of the facility.
  - ✓ When destroying diskettes, CDs and paper that contain PHI utilize shred bins.
  - ✓ Secure PHI documentation in locked bins or storage areas when you are away from your desk.
  - ✓ Use cover sheets on clip boards.
- **Security Measures**
  - ✓ Do not share Passwords with anyone for any reason.
  - ✓ Do not log someone else on the computer under your password.
  - ✓ Do not allow unauthorized students and/or observers in patient care areas.

PRIVACY

Facility Privacy Official (FPO)

- HIPAA requires healthcare entities to appoint a facility privacy official (FPO).

- The FPO in our facility oversees and implements the Privacy Program and works to ensure the facility’s compliance.

- The FPO is also responsible for receiving patient privacy complaints.

Notice of Privacy Practices

Each facility must…

- Provide Notice of Privacy Practices to patients at the first interaction.
- Inform patients of their rights and responsibilities with respect to protected health information and its uses.
- Notice is written in plain language that includes Company standard language and available in English and Spanish.
- Patient must acknowledge receipt of the notice.

Reporting Obligations

- ➢ Everyone is obligated to report any potential privacy violation that he/she witnesses or may have committed himself/herself.
- ➢ Reporting can be accomplished by any of the following:
  - ✓ An incident can be reported directly to the FPO, the Ethics & Compliance Officer or Department Manager / Director.
  - ✓ By completing a Non-Patient Notification Occurrence Report through the Risk Management System .
  - ✓ Students should report violations to their instructor.

Privacy Complaints

- FPO must maintain complaint log in accordance with the complaint process
- Privacy Complaints must be routed to the FPO
- Responses to complaints cannot be accompanied by retaliatory actions by the hospital
- Disposition of complaints must be consistent with the facility’s Sanctions for Privacy Violations

What Is My Responsibility?

- Recognize the importance of HIPAA
- Understand HIPAA Privacy and Security policies
- Handle patient information as though it were your own by utilizing shred bins when appropriate and securing it
- Stay informed – read the awareness materials and attend training
- Access all PHI at a need to know and minimum necessary basis
- "Need To Know Philosophy"- No colleague, affiliated physician or other healthcare partner, provider or student has a right to any patient information other than that necessary to perform his or her job
- Discuss potential violations or any questions with your FPO or supervisor
- Ask questions

What is Appropriate Access?

- ➢ Physicians viewing information for any of their patients and their group's patients
- ➢ Facility staff participating in the care of the patient
- ➢ Administrative processing of the patient stay
  - ✓ Peer Review
  - ✓ Patient Account Services
  - ✓ Shared Services (e.g. IT&S, Supply Chain)
  - ✓ Joint Commission

What is Inappropriate Access?

- Viewing a friend’s or neighbor’s information
- Viewing a relative’s information including spouse or child
- Viewing your own information
- Viewing paper or electronic records without a need to know
- Allowing someone to use your password

Releasing PHI

- You may release PHI without patient authorization for patient care, payment and healthcare operations (limited).

- Physicians whose names are in the medical record (those with a patient care relationship with the patient).

  For example:

  - ✓Attending Physician
  - ✓Admitting Physician
  - ✓Consulting Physician

External Faxing Guidelines

- Verify fax number
- Utilize preset numbers when applicable
- Locate fax machine in secure location
- **ALWAYS** use cover sheet with confidentiality statement for transmittals
- Highly sensitive (HIV status, mental health, abuse records, etc.) information should NEVER be faxed

Disclosing PHI to Family Members and Friends Who Call the Unit

- Patient will be assigned a four-digit pass-code
- Pass-code will be the last 4-digits of account number
- Patient will distribute pass-code to family members and friends
- May be changed during treatment, revocation form must be routed to FPO

Facility Directory

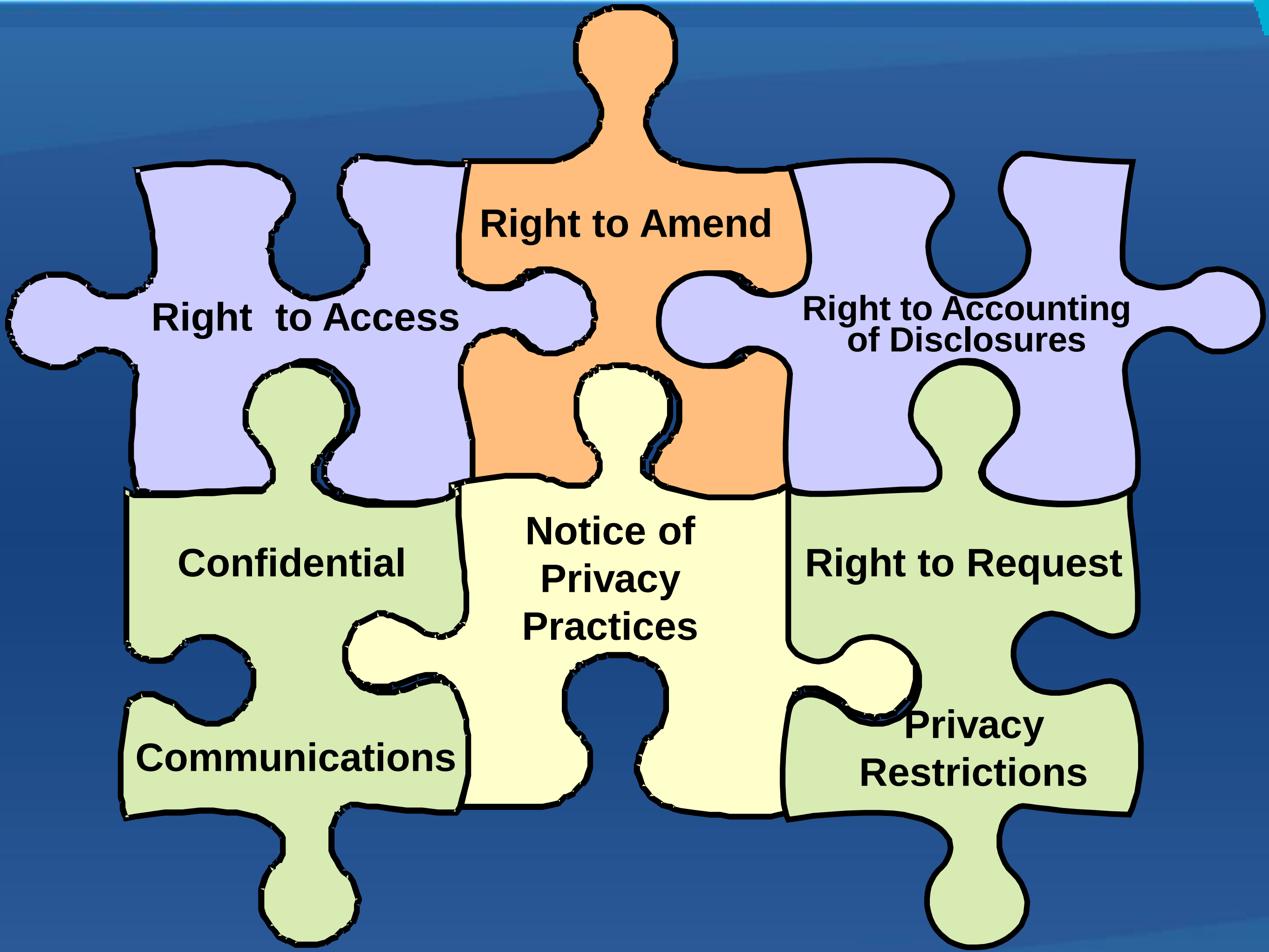
- ➢Information Desk / PBX
- ➢Opt in = Directory Information
  - ✓ Patient must be asked for by first & last name
  - ✓ Location
  - ✓ General Condition (critical, poor, fair, good or excellent)
  - ✓ Religious Affiliation (to clergy only)

Right to Opt Out of Patient Directory

- Patients have the right to opt out of being listed in the facility directory. These patients will be treated as confidential patients.
- Opt out = confidential patient notation.
- Confidential patients WILL NOT appear on directory listings at the Information Desk and PBX.
- If a patient does not appear on the directory listing individuals should respond with:

“I do not have any information regarding a patient by that name.”

Patient Rights



Right to Amend

Right to Access

Right to Accounting of Disclosures

Confidential Communications

Notice of Privacy Practices

Right to Request Privacy Restrictions

Accounting of Disclosures (AOD)

An individual has a right to receive an accounting of disclosures of PHI made by a facility in the six years prior to the date on which the accounting is requested, including:

- Required by Law
- Public Health Activities
- Judicial and Administrative Proceedings
- Law Enforcement
- Decedents
- Organ Donors
- Public Good (To avert threat to society)
- Workers’ Compensation (Non-Payment Disclosures)

Right to Request Amendment

Amend is defined as the patient’s right to add information with which he/she disagrees; record content is not to be changed or deleted.

- ➢ Request must be submitted in writing and forwarded to the FPO
- ➢ FPO must act on request to amend no later than 60 days after receipt
- ➢ If request denied, FPO must provide patient written notice outlining the reason(s) for denial

- ➢ Facility may deny patient’s request for amendment if it determines that the PHI:
  - ✓ Was not created by the Facility, unless originator is no longer available to act on the request
  - ✓ Is not part of the designated record set
  - ✓ Would not be available for access pursuant to Patients Right to Access Policy
  - ✓ Record is accurate and complete

Right to Access

- Patient has the right to inspect and obtain a paper copy of their medical record with a valid written authorization.
- Facility must act on a request for access no later than 15 days after its receipt (or provide written explanation for extenuating circumstances).
- Facility must produce PHI from its primary source or system.
- Reasonable, cost based, fees, may be imposed for copying, postage and preparing a summary or explanation, in accordance with State Law.
- Individuals with system access are not to access their own record or a family member’s record in any system. Copies will be provided with proper authorization.

Right to Privacy Restrictions

- Patients have the right to request a privacy restriction of their PHI.
- **NEVER** agree to a restriction that a patient may request.
- **All** requests must be made in writing and given to the FPO to make a decision.
- **NO** request is so small that it should not be routed to the FPO.
- Patients may request in writing that his or her health plan not be notified of an item or service paid for out of pocket.

Confidential Communications

- Request for use of alternate address or phone number for future contact which is the responsibility of the patient to provide.
- Route any request for Confidential Communications to Admissions.
- All communication only with alternate address and/or phone number given.

SECURITY

Facility Information Security Official (FISO)

- Required by HIPAA

- Responsible for compliance with all patient security laws

HIPAA Security Rule

According to the HIPAA Security Rule, our facility must take specific measures to protect the Confidentiality, Integrity and Availability of Electronic Protected Health Information (EPHI).

Confidentiality	Data or information must not be available or disclosed to unauthorized persons.
Integrity	Data or information cannot be altered or destroyed in an unauthorized manner.
Availability	Data or information is accessible and usable upon demand by an authorized person.

Why Information Security?

- Protect the availability and integrity of clinical and patient administration systems.
- Protect our patients' confidentiality.
- Maintain our facility's reputation.
- Comply with federal and state information security laws, including the HIPAA Security Rule.
- The true cost of ignoring information security is an impact to patient safety and our quality of patient care!

What Is My Responsibility?

- You play a crucial role to protect our patients and our company. You are responsible for your password by:
  - ✓ Protecting it
  - ✓ Creating quality ones
- Safely use the Internet to help protect our systems from malicious software, proper use of social networking systems (e.g. Facebook) and proper cell phone usage (no picture taking).
- Safely use email by encrypting when sending PHI outside the company.
- Recognize signs of someone attempting to illegally access our systems.
- Get help or more information about Information Security, as needed.

Protecting Against Email Viruses

- Only open email that you need to perform your job.
- Don’t open email attachments in strange or unexpected emails.
- Transmit confidential information to appropriate individuals outside the company using only approved, secure methods. (Contact your FISO if you need additional information.)
- Only use company approved software – when in doubt, ask!
- Only use company supplied diskettes or CDs.

Keeping Passwords Private

- ➢ To protect your passwords…
  - ✓ Keep them to yourself,
  - ✓ Don’t allow others to give you theirs, no matter the circumstance,
  - ✓ Never post them around your workstation
- ➢ If you suspect anyone has learned your password, change it. Call the help desk or your FISO for assistance.

Creating Quality Passwords

Keep your password safe!

- Create a hard to guess password and never share it.
- If the application allows, use a combination of special characters (like @, #, !), numbers, and upper and lower case letters.
- If the application allows, create passwords that contain at least 7 characters
- Come up with a Passphrase – Agcl2egg (All good cows like to eat green grass)

Safe Internet Use

- Only access websites that you need to perform your job.
- Be cautious about entering any company information on an Internet site.
- Do not access Internet email accounts (AOL, Hotmail, etc.) through the HCA network or from HCA computers.
- When on the Internet, use passwords and IDs that are different than your HCA ID and password.
- Never download screensavers, games, or other executable files (such as files ending in .exe, .vbs, or .com) from the Internet or any other outside source.

Social Engineering: Recognizing Con Artists

- “Social Engineers” are con artists who attempt to gain access to confidential information by deceiving you. (Beware of Phishing).
- They are good at what they do, and they know how to make you believe them. (May look official).
- They sound friendly and trustworthy, and sometimes will appear to be doing you a favor.

Possible Warning Signs

- Is someone asking you "out of the blue" questions about patient information, system names, or software?
- Has someone asked you for your password(s), or asked you to change your password(s) for them?
- Did you initiate the call/email/office visit, or did they?

Social Engineering: Outwitting Them!

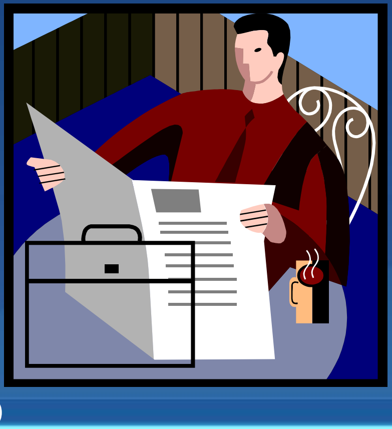
- Never give out your password over the phone.
  Even our own technical support can help you without knowing your password!
- If you didn’t initiate the contact, offer to call them back through our facility’s help desk system.
  If they claim to be part of an authorized technical support team, you should be able to call them through normal channels.
- Be aware of your surroundings.
  If you see someone you are not familiar with, politely ask their identity and ask if you can help them.
- Don't be afraid to say "No."
  If anyone asks for information such as your user ID or password, or asks you to perform a task that goes against any Company policy, just say no.
- Report it.
  If you think you have witnessed an attempted or successful security breach, report the incident to the FISO or Helpdesk immediately.

Security Awareness

- Over the past few years, we have moved rapidly into a very different world. More than ever before, we need to protect information systems.
- Our goal is to ensure the confidentiality, integrity and availability of all electronic protected health information (EPHI) the facility creates, receives, maintains or transmits.
- Information security is essential to our business. You have an essential role in our success!
- If you have any additional questions or concerns, contact the FISO, Help Desk, or another member of the facility’s IT staff.
- The security and privacy of PHI is invaluable to our patients.

What Is A Breach?

Breach occurs if there is unauthorized acquisition, access, use or disclosure of unsecured, unencrypted protected health information which compromises the security or privacy of such information and poses a significant risk of financial, reputational, or other harm to the individual.



Sanctions

Enforcement

Sanctions for Violations

Level I

Category - Accidental and/or due to lack of proper education

Violation - Failing to sign off computer
PHI in regular garbage receptacle

Recommended Action – Verbal warning with retraining

Sanctions for Violations (cont)

Level II

Category - Purposeful break in the terms of the confidentiality agreement or an unacceptable number of previous violations

Violation - Accessing a patient’s record without the need to know.
Providing information via phone without the the passcode.

Recommended Action - Written warning with retraining

Sanctions for Violations (cont)

Level III

Category - Purposeful break in the terms of the confidentiality agreement or unacceptable number of previous violations and accompanying verbal disclosure of PHI regarding treatment and status

Violation - Selling or providing patient information to a third party

Recommended Action - Termination and referral to law enforcement agency.

Civil Penalties for Non-Compliance*

Violation Category	Each Violation	All such violations of an identical provision in a calendar year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – *Corrected*	$10,000 - $50,000	$1,500,000
Willful Neglect – *Not Corrected*	$50,000	$1,500,000

Criminal Penalties for Non-compliance

- For health plans, providers, clearinghouses and business associates that knowingly and improperly disclose information or obtain information under false pretenses. These penalties can apply to any “person”.

- Penalties higher for actions designed to generate monetary gain up to;

  - ✓ $50,000 and one year in prison for obtaining or disclosing protected health information

  - ✓ $100,000 and up to five years in prison for obtaining protected health information under "false pretenses"

  - ✓ $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm

The Case of the Busy Doctor

You are a nurse at the Emergency Department nursing station, and doctor approaches you at the beginning of his rounds. The doctor needs test results for Mrs. Jones. You do not have access to Mrs. Jones' records, so the doctor wants to give you his user ID and password to print Mrs. Jones' test results.

- Where else could this happen in your facility?

  Anywhere a computer is present.

- What should you, the nurse, do?

  Suggest that the doctor use the computer in the dictation room right next to the nurses' station (or any common workstation).

- What are the possible consequences for a nurse who signs onto a system using a doctor's user ID and password? For the doctor?

  The nurse and the physician are both open to sanctions per Company policies.

The Case of the Mysterious Email Attachment

It’s Christmas time. Mary, an administrative assistant at a facility, receives an email with an attachment from Bill Brown. She does not know Bill, but his email address shows that he works for a company that has a business relationship with her department. The email subject line reads “Dancing Santa Screensaver.”

- ➢ What should Mary do with the email?

  Delete it without opening. The subject line indicates it isn’t work related anyway, so there is no reason to take the risk of getting a computer virus.

- ➢ If Mary received an email like this from a friend, what should she do?

  Again, delete it without opening. The risk of receiving a computer virus from a friend is just as great.

- ➢ If you suspect that you have opened an email that contains a virus, what should you do?

  *Notify your Facility Information Security Official (FISO), Hospital Director of Information Systems (HDIS), or other member of your facility’s IT staff immediately***.**

It Would Never Happen Here

Impacts of viruses and worms on HCA operations

- Patient safety was impacted at one facility when a worm infected and severely impacted the operation of 50 eMAR workstations due to password issues.
- Clinical operations were affected throughout the company when SQLSlammer brought down HCA’s core network for over 12 hours.
- MSBlaster worm cost HCA over $1,500,000 and 23,000 man hours of remediation effort (11.5 man years) in the first 4 weeks.
- Public knowledge of a significant security incident devalues a company’s stock by an average of 5.5% within the first 3 days. For HCA, this represents a loss of over $1.09 billion in shareholder value.

Confidentiality

The delicate balance between all stakeholder’s need to know and the patient’s right to privacy is at the heart of HIPAA.

Protection of Patient Privacy & Security

All stakeholders (patient and non-patient care areas) are obligated to protect patient privacy and security rights! This includes health information in ANY form or media (i.e., electronic, paper, oral, CD, diskette, and microfilm).

Contact Information

- FPO – Christine Hess (956) 350-772
- FISO - Carlos Leal (956) 632-6123