Privacy Regulations Provider CME

HIPAA

HITECH

New Hampshire State Laws

HIPAA: What is it?

- HIPAA is the Health Insurance Portability and Accountability Act (HIPAA), is a Federal Law that was enacted in 1996.

- Congress passed HIPAA to improve the health care system in the United States to create efficiencies through the use of electronic transaction.

HIPAA Rules

- To implement the statutes the US Department of Health and Human Services has published a series of rules including but not limited to:
  - Privacy Rules – govern the confidentiality of protected health information
  - Security Rules – governs the security and confidentiality of health information in electronic form

HIPAA Intent

- To reform the healthcare industry by:
  - Reducing cost
  - Simplifying administrative processes and burdens
  - Improving the privacy and security of patient information

HITECH Act: What is it?

- Health Information Technology for Economic and Clinical Health Act was enacted as part of American Recovery and Reinvestment Act on February 17, 2009.

HITECH Intent

- Electronic Health Records (EHRs) Implemented Nation Wide
- Reduce Waste
- Prevent Medical Errors

HITECH Financial Incentives

- To qualify you must use a “certified” EHR
- “Certified” is yet to be defined, but must:
  - Protect PHI
  - Ensure comprehensive demographic and clinical data
  - Include patient demographics and clinical health information
  - Should have the capacity to provide clinical decision and physician order entry

HITECH Highlights

- Provisions for increasing patient rights
  - Limiting Marketing
  - Breach Notification
  - Security of Protected Health Information (PHI)
- Changes for Business Associates
  - Accountability for Protection and Security of PHI
  - Penalties for Non-Compliance

HITECH Highlights

- Minimum Necessary Rule
  - Effective August 2010
- Electronic Medical Record (EMR) Accounting of Disclosure
  - Effective January 2011
- Sale of (Records) Protected Health Information
  - Effective April 17, 2011

HITECH
What is a Breach ?

- The unauthorized acquisition, access, use, or disclosure of unsecured protected health information which compromises the security or privacy of such information.
- Includes: electronic, verbal and paper
- September 2009

HITECH
Breach Notification

- When a breach is discovered each individual needs to be notified within 60 days.

- Specific requirements must be met
  - Description, date, time discovery, steps taken to protect, investigative process, future prevention, provide toll free number, e-mail address, website, postal address and where to receive additional information.

HITECH
Breach Notification Process

- Greater than 500 individuals
  - Notice without reasonable delay; 60 days and be in the form of the press release
  - DHHS notified at the time the individuals are notified
- Less than 500 individual
  - Maintain a log
  - Submit to Secretary of DHHS at the end of the calendar year
- If less than 10 Individuals or Contact Information Inadequate
  - Substitute notice may be utilized

HITECH Breach Penalties

- Individuals who breach HITECH can be penalized by the Department of Justice

Violation	Each Violation	All such within the same 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	$1500,000

NH State Law (RSA 359-C:20) What is a breach?

- Personnel information that encompasses:
  - First name, last name

  and

  - A combination of social security number, drivers license, credit card debt numbers, that potentially could permit access to individual's financial account access.

NH Law RSA 359-C:20

- Notification Requirements of a Security Breach:
  - Written
  - Electronic (if primary means)
  - Telephonic (must keep a log)
- Substitute Notice may be given by e-mail posting on web site, or major state wide media if:
  - cost exceeds $5000
  - or if breach exceeds 1000 individuals
  - or if contact information is limited

NH Law RSA 359-C:20

- Notice includes:
  - General Description
  - Date of Breach
  - Type of Information
  - Where Affected Party Can Call
  - Notice Needs to Comply with HIPAA

- If more than 1000 individuals are affected then you must also notify all consumer reporting credit agencies without delay (notices do not need to include names of affected parties)

What Is a “Business Associate ?”

- A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services, to a covered entity.

HITECH
Business Associate

- Provisions that are incorporated into the business associates regulations:
  - Civil and criminal penalties are added.
  - May not use or disclose PHI except for in accordance with Business Associate Agreement terms.

Restriction on Minimum Necessary HITECH

- Must comply with individual requests to restrict disclosure:

  (1) to health plan for healthcare operations

  (2) for items/services for which provider was paid in full "out of pocket"

Guidance expected August 2010

HITECH
Accounting for Disclosure

- Must comply with individual requests to restrict disclosure

- Patient may refuse disclosure for healthcare operations
  - This pertains to items/services for which the individual pays the provider in full “out of pocket”

Guidance pending August 2010

HIPAA
Marketing and Fundraising

Regulations prohibit the use of PHI for Marketing unless the patient signs a specific authorization.

Exception:

Physicians may discuss products and services in face to face encounters, however the physician must disclose any financial relationship when referring patients.

HIPAA
Fundraising

- Patients must be informed on how to opt out of fundraising communications.
  - You can not abstract patient's data i.e. diagnosis, surgical procedure categories for fundraising, u*nless a specific authorization is obtained .*

New Hampshire RSA 332 -1 Limiting Fundraising

- Fundraising must include a clear and conspicuous “opt out” option.
- This option must be given 60 days prior to receiving fundraising communications.

New Hampshire RSA 332 -1 Limiting Marketing

- Marketing is defined as:
  - a communication about a product or service that encourages individuals to purchase or use the product or service
- Marketing communications are not healthcare operations
  - Examples of healthcare operations:
    - treatment, case management, care coordination, alternative therapies, and providers of care

Privacy Regulations

Situations to be aware of:

High Risk Situations

- Public Areas – Avoid discussion in public areas. Always be aware of where you are and exercise discretion.

- Friends and Families – You are not permitted to review the medical record of your friends and families.

High Risk Technology

- Face book – *Posting the image of a patient without authorization is an inappropriate disclosure*
  - Twitter or Blogging - (is to read, write, or edit and share an on-line journal)

When individuals are in the news it becomes easy to identify even if the name is not utilized

High Risk Technology

- E-Mails that contain PHI if sent out of the SJH system must to be encrypted.

- Texting PHI between clinical providers:

  Text messages are not encrypted and may be read by anyone accessing your telephone

Notice of Privacy Practices

- Privacy Notice needs to be posted in the office and on your web page.

- Privacy Notice needs to be handed out to the patient.
  - It informs patients about their rights to obtain copies of their record, view their record, and request amendments.
  - Instructs the patient how to file a complaint with the organization and DHHS.

Amending a Record

- Patients are increasingly viewing their medical records.
  - A patient may request a record be amended.
  - The Medical Records Department and the Privacy Officer will process the request.
  - A provider may be asked to amend your note in a record.
  - A provider may decide not to amend the record, but the patient has the right to attach their own statement.
  - SJH employee refer to Policy HIM-15

Patient Contact Information

- A patient might request communication (mail or test results) to be directed to an alternative address, phone number etc.
- This should be documented in the record and followed.

Examples of Permitted Disclosure of PHI without Authorization

- Patient location in the hospital (patient has the right to opt out)
- Reporting information to Public Health Agencies
- Reporting to the FDA on medical devices
- Reporting Child and/or adult abuse, domestic violence
- Reporting of suspicious deaths
- Responding to certain military requests

Special Circumstances for Release of PHI without Authorization

- In some situations a court order, or a subpoena from law enforcement maybe required to release without authorization
- These special circumstances must be reviewed by the Practice Office Manager
- Director of Risk Management may be contacted as necessary

Release of PHI to Families/Friends Involved in Care

- Permission from the patient is required before discussion of the patient care and treatment with family members, friends etc.
  - Exception 1
    - If the patient is not able to grant permission (i.e. patient unconscious) and the provider believes it is important to discuss certain information about the patient, such discussion is permitted and should be documented.
- SJH employee refer to Policy HIM-08

Release of PHI to Families/Friends Involved in Care

- Exception 2
  - When a patient is actively being treated, information can be released if the patient was offered the opportunity to object to such release and does not object.
  - This must be documented.

Release of PHI to Families/Friends Involved in Care

- Minors in the Military and/or married minors may consent for their own healthcare.
- Minors 14 years and older may consent for Sexually Transmitted Disease Testing and Treatment.
- Minors 12 years and older may consent for Drug and Alcohol Testing and Treatment.
- If a minor is able to consent for treatment, then the minor can release their PHI.
- SJH employee refer to Policy PR-01

Families/Friends Involved in Care

- If a minor has been the victim of domestic violence, abuse, and/or neglect by parent or guardian and the release to this party would endanger the minor then release of information should be reviewed by the Practice Office Manager.

What you need to do for Security

- Manage your passwords
- Prevent the spread of virus
  - For example i.e. don’t open an e-mail from unknown sources
- Log off your computer
- Assure that patient information access is restricted

What SJH does:

- Responds to occurrences that involve security
- Monitor login attempts
- Protect computers from malicious attacks and viruses
- Conduct security audits and access to PHI
- Has role based PHI access
- Conducts data recovery

Your assistance is needed to:

- Assure that computer screens are not visible to the public
- Ensure laptops and personal devices (Blackberries, I Phones) are secure
- Secure disks, and USB's when not in use
- Be aware of the HIM policies
- Use screen savers, and passwords
- Always be aware of your surroundings