HIPAA & HITECH

Privacy, Security, Breach Notification & NYS Confidentiality Laws

SDM Training

Stephanie Musso, SBUH HIPAA Privacy Officer & Director Information Security

H = Health

I = Insurance

P = Portability – *NOT PRIVACY*

Created to ensure access to health coverage

Allows for continuity in health coverage

Prevents denial due to a pre-existing condition(s)

A = Accountability

Healthcare fraud is a federal crime

Fines and/or jail time may apply Individuals

Organizations could face sanctions

A = Act

Privacy and Security Rules added following extensive lobbying by Privacy Advocates

HIPAA

What is PHI ?

Any form of information that can identify, relate or be associated with an individual obtaining health care services

What is IIHI?

Individually **I**dentifiable **H**ealth **I**nformation are data elements that make up **PHI** such as……

Name, Address, SSN, Phone Number, Medical Record Number, Diagnosis, Test Results, Photographs, Doctors notes, Health Plan Information, etc.

With advances in technology come the potential for misuse and abuse.

Electronic storage of data

E-mail

World Wide Web

All easily allow information to travel outside the organization.

Why is there a need for this added protection ?

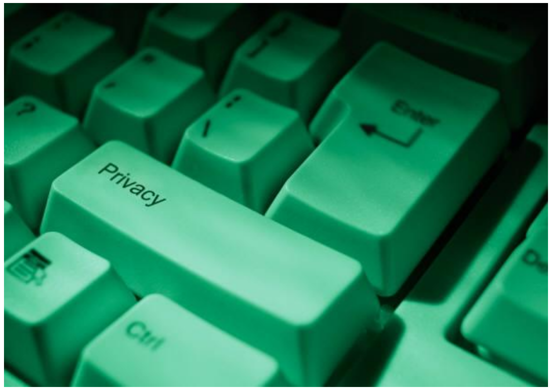
All manners of communication containing PHI including:

At all times

Spoken

Written

Electronic



To Provide Care:

Healthcare providers/practitioners can share PHI for continuity of care.

Obtain payment:

Billing a medical insurance company for service rendered or providing the patient’s name & address to a collection agency

Health Care Operations:

Quality Improvement, teaching & education, legal proceedings, certification or accreditation processes, etc.

When are we permitted to share PHI?

1) Maintain our patient’s trust

Improve patient safety & patient satisfaction

2) Safeguard our patient’s **PHI**

Required by the HIPAA Security Rule

3) Educate our patients as to their rights.

Required by the HIPAA Privacy Rule

What are our Privacy Goals ?

Stony Brook Organized Health Care Arrangement (SBOHCA)

a.k.a

JOINT NOTICE OF PRIVACY PRACTICES

Is the document SBUH uses to notify patient's of their privacy rights…

> request restricted use and disclosure of PHI*

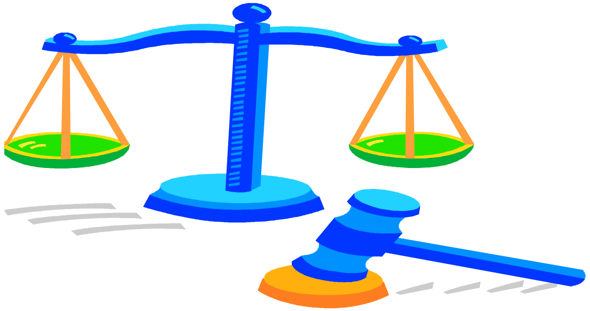
> request to receive communications via alternate mechanism

> inspect and copy their health information*

> request to amend their medical record

> request an accounting of disclosures*

> file a complaint*



PATIENT’S RIGHTS

Information Security is the process of protecting data from accidental or intentional misuse by persons inside or outside of the Hospital

Set standards to ensure **only those who should have access to PHI** contained in the electronic systems actually have access and **ensure the integrity of our PHI** in the electronic systems is maintained

Protected Health Information contained in our electronic systems is better known as **e-PHI.**

HIPAA Security Rule

- **Administrative Safeguard (policies, training, audits, etc.)**

- **Physical Safeguards (locks, privacy screens, etc.)**

- **Technical Controls (firewalls, encryption, virus protection, etc.)**

Note: The Federal HIPAA Security Regulation requirements are in alignment with the NYS Cyber & Information Security Law, TJC standards & the NYS DOH Regulations

HIPAA Information Security Requirements

On February 17, 2009 the Federal Stimulus Bill or American Recovery and Reinvestment Act (ARRA) was signed into law and included provisions to address Health Information Technology For Economic and Clinical Health Act (HITECH).

Purpose is to create a *national health information infrastructure* and widespread adoption of electronic health records through monetary incentives.

Provide enhanced Privacy & Security Protections under HIPAA including increased legal liability for non-compliance and greater enforcement actions.

*H*ealth *I*nformation *T*echnology *E*conomic & *C*linical *H*ealth

Breach Notification (PHI sent/given to the incorrect recipient)

Patients can request an **Electronic Copy** of their medical Info.

Individually Directed Privacy Restrictions

Restrictions on Marketing, Fundraising and the **sale of PHI**

Preference for **Limited Data Sets and De-Identification**

Extension of **Minimum Necessary Rule** (use & access)

Vendors/Business Associates (subject to the same penalties)

Accounting for Disclosures (access lists)

Increased Enforcement and New Penalties - *Individual's & Organizations* are subject to the criminal provisions; **State AG's** can bring civil suit in Federal Courts on behalf of state residents; ***harmed individuals can receive a % of CMP's or settlement***

What changes should we expect?

Stricter State Laws that surpass HIPAA:

Article 27-F NYS PHL

Confidentiality of HIV – related information

NYS MHL

Confidentiality of mental health information applicable to OMH certified providers & locations

Genetic Information Non-Disclosure Act (Fed & NYS Law basically the same) protects potentially harmful disclosures of genetic information

Use, Access and Disclose the minimum necessary to perform your assigned responsibilities (provide treatment to a patient; obtain payment for the services rendered; or perform a healthcare related function or operation as assigned (QA/QI, audit, care management/ utilization review, teaching, etc. definitions can be found Admin P&P LD: 0075)

Do Not Snoop even if they beg

(neighbors, friends, relatives, immediate family members, ***colleagues***)

Dispose of PHI properly and ensure PHI that is sent electronically is sent to the proper recipient

Notify the HIPAA Privacy Officer if you misdial a fax # and send PHI to the incorrect recipient or mail patient information to the wrong address.

When in doubt ask the HIPAA Privacy Officer phone 4-5796 or e-mail "HIPAA"

As an employee what is expected of me ?

Remember your username and password are your signature:

Do Not Share usernames/passwords; Do Not use a generic sign-on

Log-Off before walking away from a workstation

Do not place patient information on mobile devices

Do not post patient information on Social Network sites

Do Not take pictures of patients with non approved devices and without patient consent

Do not install/download on a SBUH computer without IT approval

When sending patient information via e-mail use only SBUH Outlook and send only to another SBUH Outlook user only. Remember send the ***minimum necessary*** amount of information needed, ensure you have the correct recipient and when in doubt contact Information Security phone 4-5796 or email “Information Security”

As an employee what is expected of me when using electronic information?