HIPAA

Department of Health Care Services

(DHCS)

Introduction

- HIPPA stands for **Health Insurance Portability and Accountability Act**.
- passed by Congress in 1996.
- **HIPPA does the following:**
- Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs.
- Reduces health care fraud and abuse.
- Mandates industry-wide standards for health care information on electronic billing and other processes.
- Requires the protection and confidential handling of protected health information

Introduction

HIPAA -- IT compliance.mp4

What is HIPAA.mp4

Rules

- The Privacy Rule, which sets national standards for when protected health information (PHI) may be used and disclosed

- The Security Rule, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI)

- The Breach Notification Rule, which requires covered entities to notify affected individuals, U.S. Department of Health & Human Services (HHS), and in some cases, the media of a breach of unsecured PHI

Rules (Examples)

- Do not discuss patient's care with anyone not directly involved.
- Do not discuss patient details with family, friends, etc.
- Do not talk about patient in public areas.
- Do not read patients' charts when you are not involved in their care.

The HIPAA Compliance Audit Program

- In 2011, the Office for Civil Rights commenced a series of pilot compliance audits to assess how well healthcare providers were implementing HIPAA Privacy, Security and Breach Notification Rules. The first round of audits was completed in 2012 and highlighted the dire state of healthcare compliance in America.
- Audited organizations registered numerous violations of the HIPAA Breach Notification Rule, Privacy Rule and Security Rule, with the latter resulting in the highest number of violations.

The HIPAA Privacy Rule

What is the HIPAA Privacy Rule?

- What is PHI?
- Use and Disclosure of PHI
- Marketing and Fundraising Protocols
- Patient Access to Medical Records
- Notice of Privacy Practices

- NOTE: The HIPAA Privacy Rule applies to PHI in any form. This includes computer and paper files, x-rays, physician appointment schedules, medical bills, dictated notes, conversations, and information entered into patient portals.

HIPAA regulations list eighteen different personal identifiers (PHI):

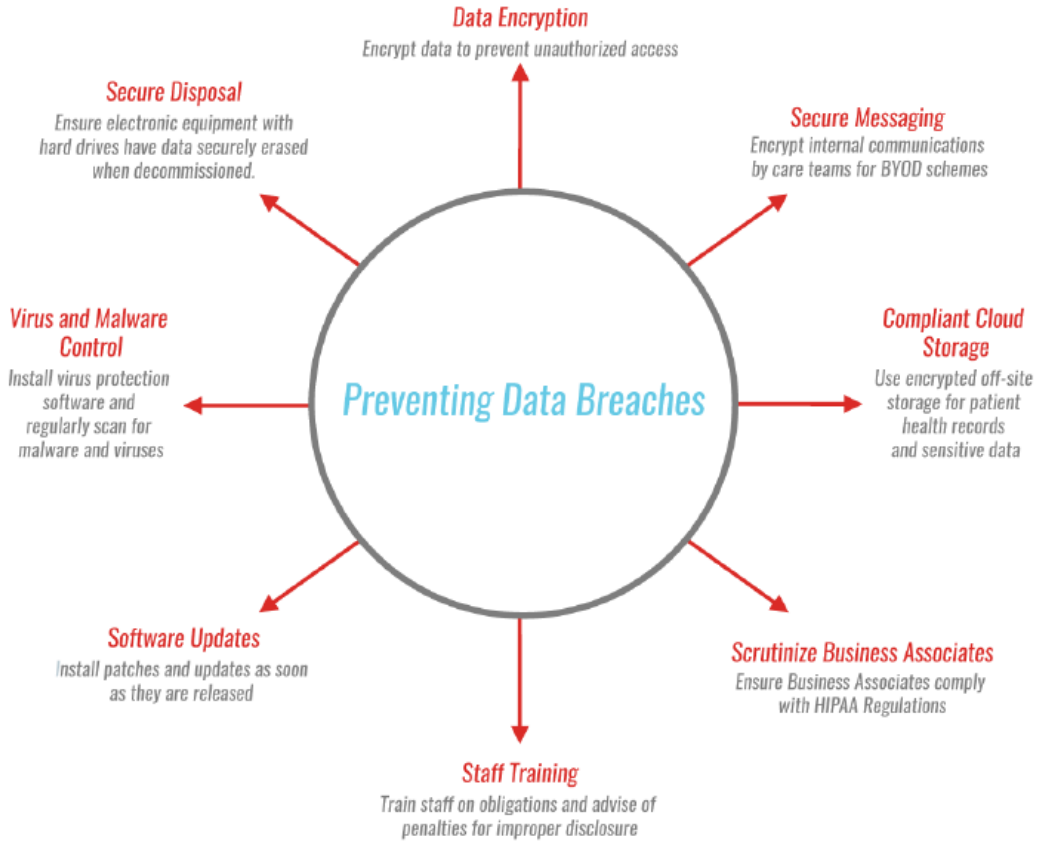
- Names
- All geographical data smaller than a state
- Dates (other than year) directly related to an individual
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance plan beneficiary numbers
- Account numbers

Eighteen personal identifiers are:

- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Device identifiers and serial numbers
- Web URLs
- Internet protocol (IP) addresses
- Biometric identifiers (i.e. retinal scan, fingerprints, Etc.)
- Full face photos and comparable images
- Any unique identifying number, characteristic or code

Notice of Privacy Practices

- An example of a Notice of Privacy Practices can be found on the OCR´s website



The HIPAA Security Rule

- What is the HIPAA Security Rule?
- What is the Difference between PHI and ePHI?
- Technical Safeguards
- Physical Safeguards
- Administrative Safeguards
  - Policies, Sanctions and Training
  - Contingency and Disaster Recovery Plans
  - Risk Analysis and Risk Management

What are the HIPAA Requirements for a Website?

- Transport Encryption: Data must be encrypted if it is transmitted over the Internet
- Backup: Data cannot be lost, I.e. it should be backed up and must be recoverable
- Authorization: Data can only be accessible by authorized personnel using unique, audited access controls
- Integrity: Data cannot be tampered with or altered
- Storage Encryption: Data should be encrypted when it is stored or archived
- Disposal: Data must be permanently erased when it is no longer needed
- Sharing: If data is located on the web servers of a third party, that entity must agree to comply with HIPAA regulations and a HIPAA Business Associate Agreement must be in place

How Does a Simple Website Stack up Against These Requirements?

- By a simple website, we refer to one set with any of the popular hosting providers (e.g. GoDaddy) and written using off the shelf software or by someone without training in HIPAA website security best practices:
- Transport Encryption – Fail
- Backups – Uncertain
- Authorization – Uncertain
- Integrity – Fail
- Storage Encryption – Fail
- Disposal – Uncertain
- Business Associates – Fail

oTHER SECURITY CONCERNS

- IT Network Security
- Text Messages and Replacing Pagers