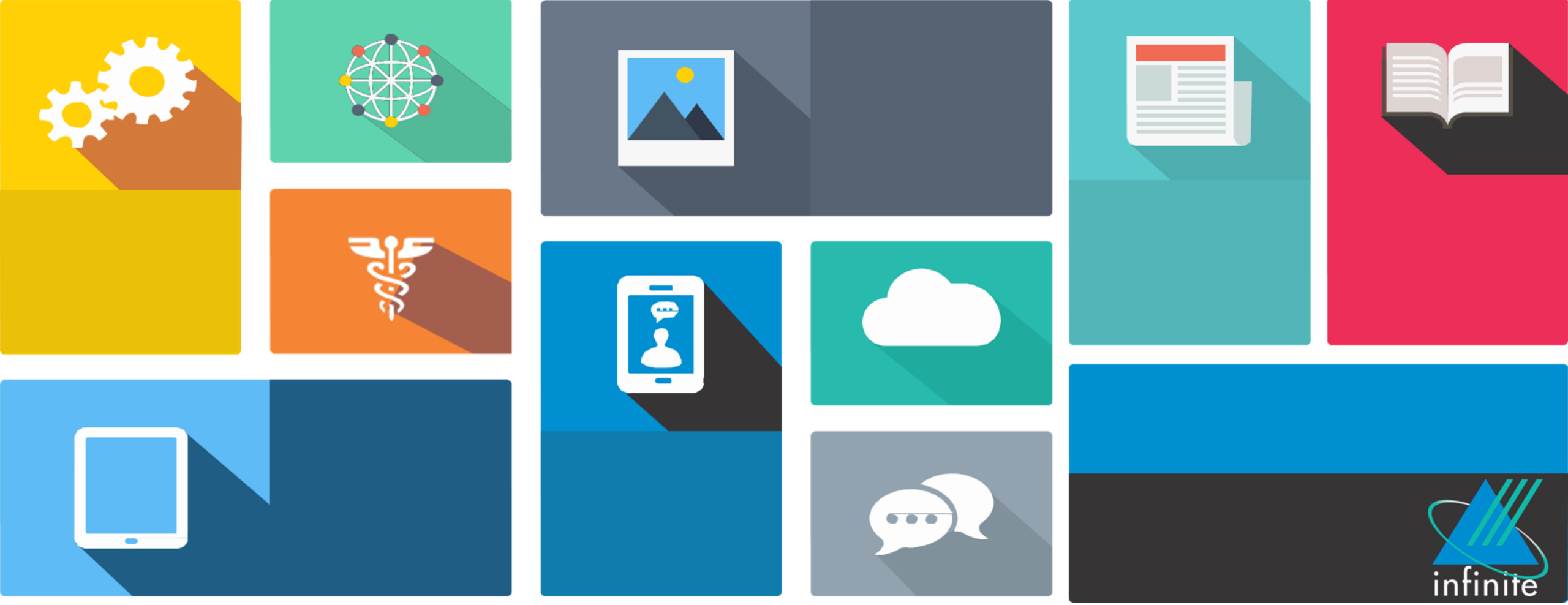


HIPAA AWARENESS & SECURITY TRAINING

© 2018 Infinite Computer Solutions . All Rights Reserved

What is HIPAA?

It is a federal law enacted in 1996 as an attempt at incremental health care reform.

HIPAA's intent is to reform the health care industry by

- Reducing costs
- Simplifying administrative processes and burdens
- Improving the privacy and security of patients' information

Who is affected by HIPAA?

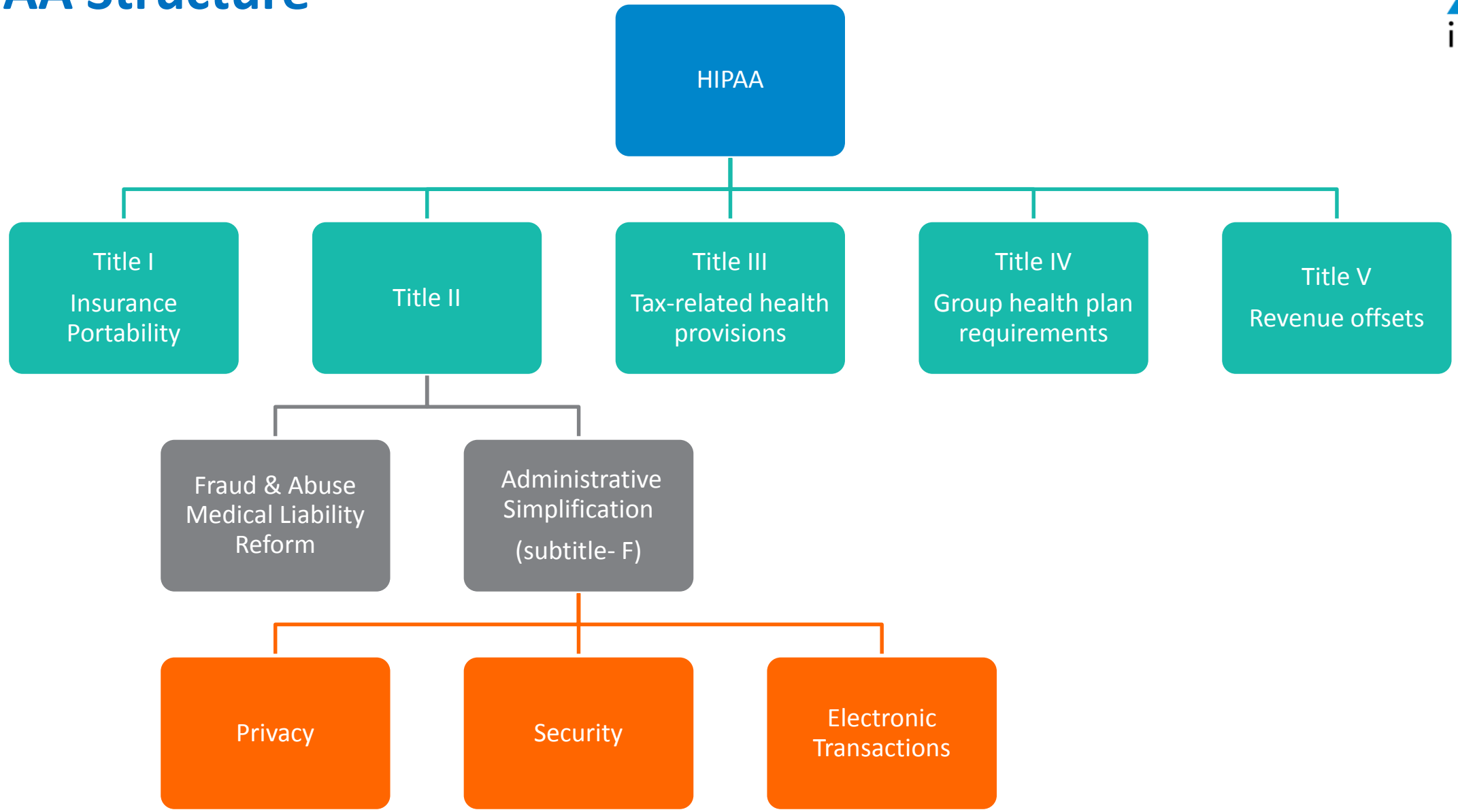
Directly Affected

- All organizations that directly maintain and transmit protected health information.
- These include health care providers, hospitals, physician practices, dental practices, health plans, laboratories, health care clearinghouses, pharmacies, etc.

Indirectly Affected

- All third party vendors and business partners that perform services on behalf of or exchange data with those organizations that directly maintain and/or transmit protected health information.
- Examples are accountants, lawyers, medical answering services, consultants, billing agencies, etc.

HIPAA Structure

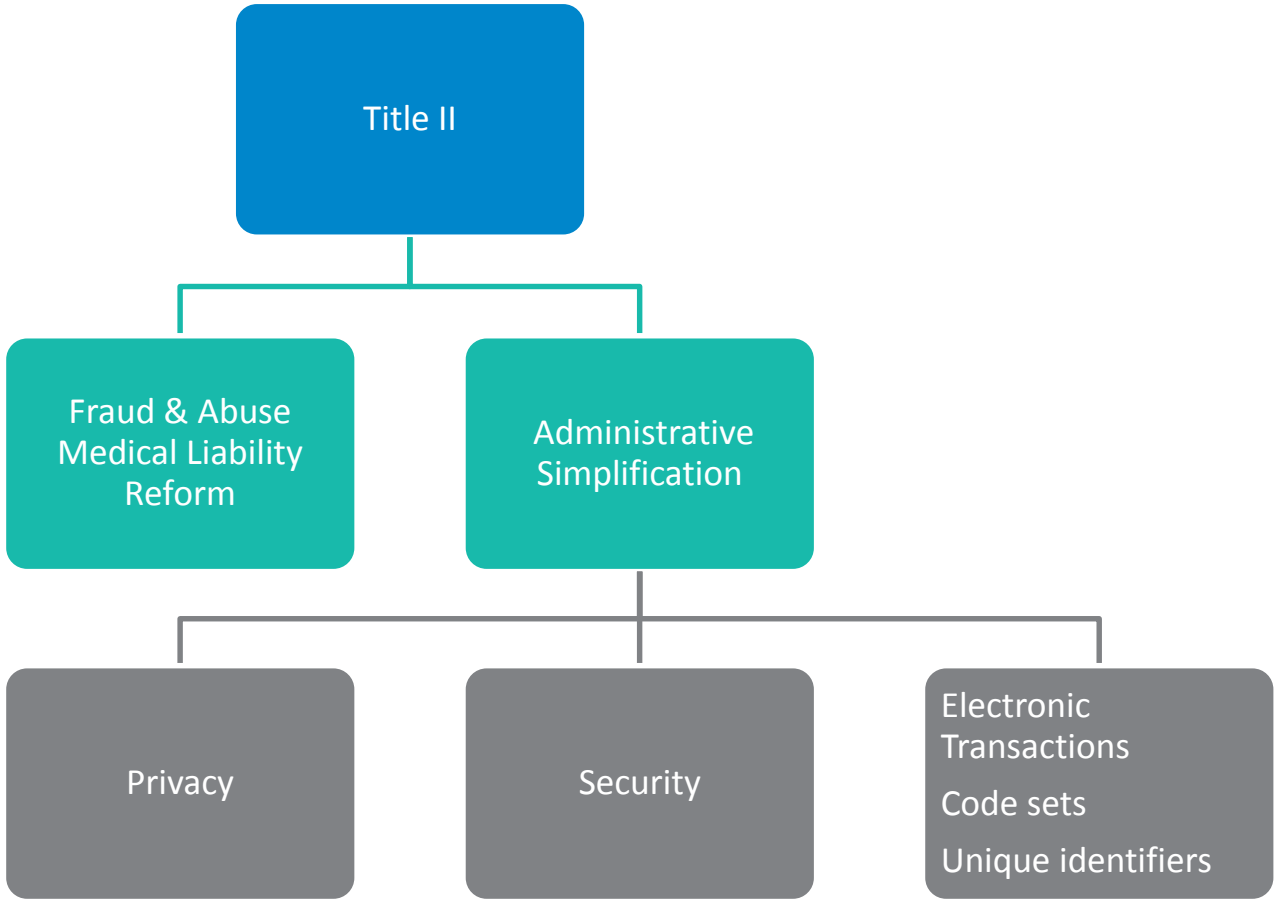


Title I – Health Insurance Access, Portability, and Renewability

- Provides limitations on pre-existing condition exclusions
- Prohibits discrimination against individuals based on health status
- Helps individuals to keep health insurance when they change jobs
- Prevents insurers from imposing pre-existing condition exclusions on new members when they have prior creditable coverage
- Guarantees that once employers or individuals purchase health insurance, those policies will be renewed

Title II – Preventing Health Care Fraud And Abuse

The Administrative Simplification section of HIPAA consists of standards for the following areas:



Fraud & Abuse Medical Liability Reform

- Created Fraud & Abuse Control Program and Medicare Integrity Program
- Created incentives for beneficiaries to report suspected fraud & abuse
- Established penalties for program violations:
  - Fines and returns of overpayments
  - Criminal prosecution
  - Exclusion from federal healthcare programs
- Mandated national data collection effort on fraud & abuse
- Defined Civil Monetary Penalties (CMPs) for violations
- Revised criminal laws relating to healthcare fraud

Administrative Simplification – Privacy Rule

- Designed to protect an individual's health information that is held by HIPAA covered entities and their subsequent business associates (BAs)

- Individually Identifiable Health Information
  - Health information, including demographic information
  - Relates to the individual's physical or mental health or provision of, or payment for health care
  - Identifies the individual

"The member who asked to review his claims and payments, requests an amendment to his record. The diagnosis given on the claims is Hepatitis B, but the member states he was treated for Hepatitis A. The Privacy Officer reviews the medical records from the provider and indeed finds the claim was miscoded. An amendment is made to the record and a note made on each claim with the incorrect diagnosis that references the amendment."

Administrative Simplification – PHI

Protected Health Information (PHI) – Some examples

- Name
- Address including city and zip code
- Telephone number
- Fax number
- E-mail address
- Social security number
- Date of birth
- Medical record number
- Health plan ID number
- Dates of treatment
- Account number
- Full face photo and other comparable image
- Certificate/license number
- Device identifiers and serial number
- Provider ID number
- Vehicle identifiers and serial number
- Application Tracking Number
- Internal Control Number
- URL
- IP address
- Biometric identifiers including finger prints

Privacy Rule – Example

CVS pharmacy – January 2009, $2.25 million

Individuals affected: OCR investigation, launched in response to media reports on the topic, found several CVS Pharmacies were disposing of Protected Health Information in public dumpsters. In collaboration with OCR, the Federal Trade Commission also launched an investigation into CVS. Officials determined the pharmacy chain did not have adequate policies and safeguards in place to protect patient data and dispose it of in the proper way.

Cignet Health Center – 2010, $4.3 million

Individuals affected: – Maryland based health center from 2008 – 2009 denied 41 patients requests for their medical records, for which the medical group practice was fined $1.3 million. Moreover, during the investigation into Cignet allegations, the practice subsequently refused to respond to several of OCR demands to produce their records and failed to cooperate with investigation requests, OCR officials said. For this, the practice was fined $3 million.

Administrative Simplification – Security Rule

- Complements the Privacy Rule
- Deals specifically with E-PHI
- Lays out three types of security safeguards required for compliance

Administrative	Physical	Technical
• Security Management Process • Information Access Management • Workforce Training and Management • Evaluation	• Facility Access Controls • Workstation Use • Workstation Security • Device and Media Controls	• Access Control • Audit Controls • Person or Entity Authentication • Transmission Security

Administrative Processes – Example

New York and Presbyterian Hospital (NYP) and Columbia University, $4.8 million.

- In a joint case, the two organizations were fined after 6,800 patient records were accidentally exposed publicly to search engines. The breach was caused by an improperly configured computer server that was personally owned by a physician. The server was connected to the network that contained ePHI.

- NYP lacked processes for assessing and monitoring all its systems, equipment, and applications connected with patient data. It also didn't have appropriate policies and procedures for authorizing access to patient databases. Both of these violations would have been easy to prevent through administrative processes.

Physical Processes – Example

Scenario

- Lily, a nurse who works on 5-West, has a lot of access to PHI.
- Tara, a nurse who works on 4-North, learns that her friend and elderly neighbor, Ms. Pate, was admitted to 5-West.
- Tara is concerned and wants to help so she asks Lily to see Ms. Pate's medical record. Together, they review and discuss their findings.
- Is this a HIPAA violation? If so, what did the healthcare professionals do wrong?

Technical Processes – Example

University of Mississippi Medical Center (UMMC), $2.75 million

- UMMC reported a breach after a password-protected laptop loaned to a visitor went missing. Subsequently, OCR's investigation found that users could access a network drive containing ePHI via a wireless network with a generic user name and password. The accessible network drive contained ePHI of 10,000 patients dating as far back as five years.

- According to Verizon's 2016 Data Breach Investigations Report, more than 60 percent of data breaches in 2015 involved weak, stolen, or default passwords. Passwords are a major problem that can have serious consequences for organizations, yet it's a problem that's easy to mitigate by implementing strong password-management policies as well as techniques like multi-factor authentication.

HIPAA Security – The “Do and Don’t”

Do Not’s

- Install unauthorized software (e.g. screensavers, games, or instant messenger programs)
- Install any unlicensed software on your computer or device
- Abuse your Internet or e-mail access privileges
- Relocate any computer equipment without prior approval
- Bring in any personal computer equipment without prior approval (e.g. Pen drive, digital / mobile cameras)

Security concerns should be reported to Compliance officer

- Unauthorized or suspicious visitors
- Logged-on but unattended workstations
- Uncontrolled access to areas that house equipment and/or PHI
- Passwords on Post-it notes
- Accessing records without a need to know

Administrative Simplification – Electronic Transactions

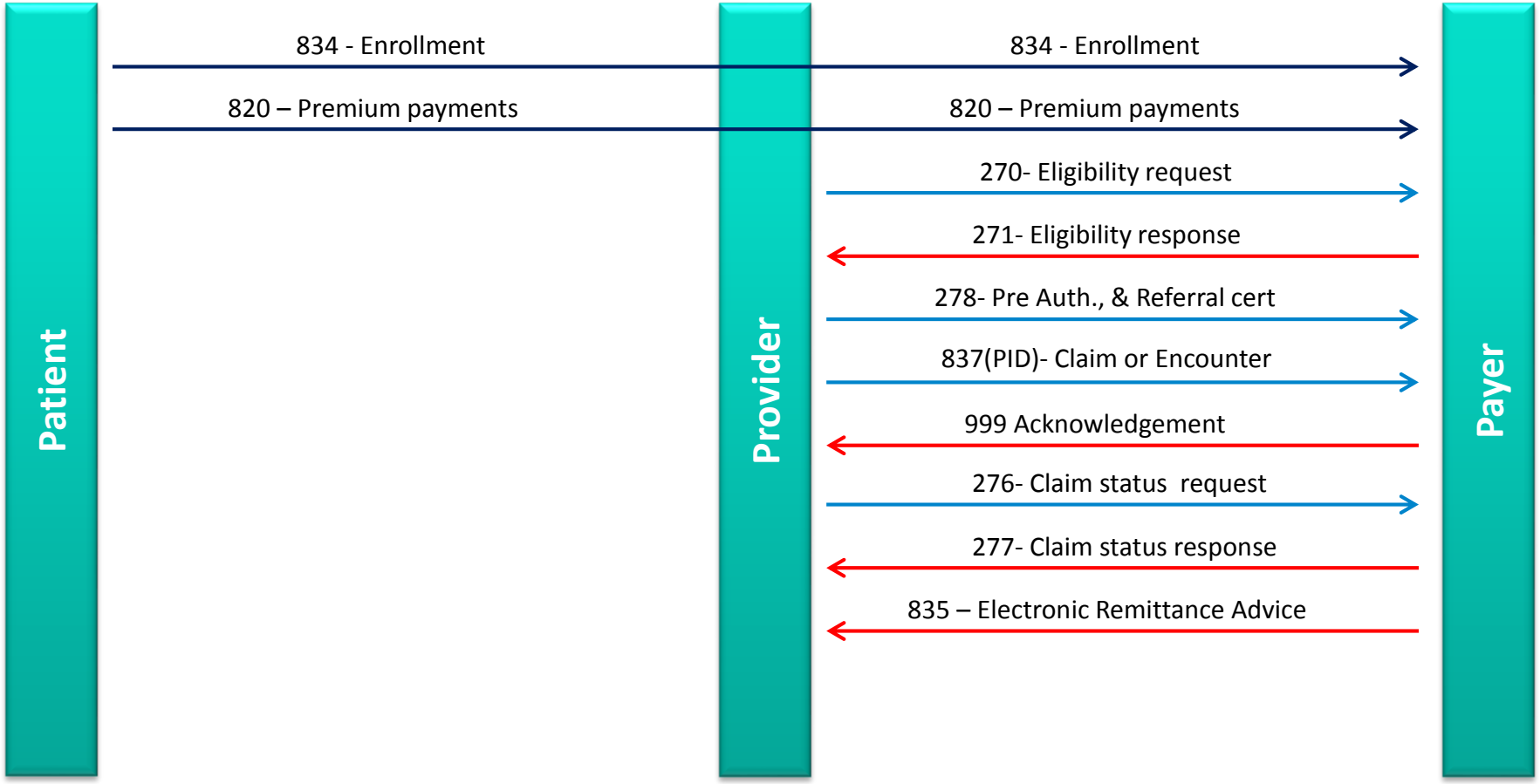
Transactions and Code Sets Rule

CMS announced that after July 1, 2005 most medical providers that file electronically will have to file their electronic claims using the HIPAA standards in order to be paid

EDI transactions

- EDI Health Care Claim Transaction set (837)
- EDI Retail Pharmacy Claim Transaction (NCPDP Telecommunications Standard)
- EDI Health Care Claim Payment/Advice Transaction Set (835)
- EDI Benefit Enrollment and Maintenance Set (834)
- EDI Health Care Eligibility/Benefit Inquiry (270)
- EDI Health Care Eligibility/Benefit Response (271)
- EDI Health Care Claim Status Request (276)
- EDI Health Care Claim Status Notification (277)

EDI Transactions



Code Sets

Adopting a uniform set of medical codes is intended to simplify the process of submitting claims electronically and reduce administrative burdens on health care providers and health plans.

- ICD 9 & 10 Codes
- HCPCS and CPT codes
- NDC Codes
- Revenue Codes

Administrative Simplification – Unique Identifiers Rule

Unique Identifiers Rule (National Provider Identifier)

- NPI is 10 digits (may be alphanumeric), with the last digit being a checksum.
- Use of the NPI to identify covered healthcare providers
- Replaces all other identifiers used by health plans, Medicare (i.e., the UPIN), Medicaid, and other government programs
- Does not replace a provider's Drug Enforcement Act (DEA) number, state license number, or tax identification number

Title III – Tax Related Provisions

- Established non-taxable Medical Savings Accounts (MSA) to pay medical bills

To qualify for a tax-preferred MSA:

	Individual	Family
Deductible	$1,500 - $2,250	$3,000 - $5,000
Out-of-pocket limit	$3,000	$5,500

- The individual or family account holder cannot be covered by any other insurance, except that which is specifically allowed under this section.

Example

Example

- Sara has a $2,000 deductible insurance plan. She deposits $2,000 into an MSA account.
- Sara has a healthy year, seeing the doctor twice for office visits when she has a cold and slight fever for which she gets prescription medications. Each office visit costs $35, and the drugs cost another $25 each time, for a total of $120.
- She pays these expenses from her MSA, leaving a balance of $1880. It carries over into the next year, when she deposits a new $2,000. With the deposit, Sara will have a total of $3,880 for medical bills for the second year. Meanwhile, the account is growing because she has placed the money with a bank, where it is in an interest-bearing savings account.

- The money accumulates tax-free, and Sara can withdraw it at any time for medical costs. If the money builds up, it can ultimately serve as a retirement health account. She can use it to pay Medicare premiums, or to pay for long-term care insurance or nursing care, or any other expenses that might arrive along with old age

Example

Example

- Bob who also has a $2,000 deductible and opens a $2,000 account. But Bob isn't as lucky with his health. He undergoes surgery and has a slow recovery, and has a total of $75,000 in medical bills for the year. The coverage provides for 80% payment by his insurance plan and 20% payment by Bob. He pays the first $2,000, his deductible, and then withdraws the $2,000 from the MSA.

- For the remaining $73,000 in medical bills, Bob’s 20% share would be $14,600. However, remember that the out-of-pocket limit for insurance with an MSA is $5,250. Bob spends $3,250, because he has already paid $2,000, reaching the limit for his personal outlays. All the rest of the money, $69,750, would be paid by the insurance plan.
- Next year, Bob starts fresh with a new $2,000 deposit into his health savings account.

Title IV – Application & Enforcement of Group Health Plan Requirements

- Employer-sponsored group health plans must offer certain employees and their dependents option of purchasing continued health coverage in the case of certain qualifying events

Qualifying events include:

- termination or reduction in hours of employment,
- death, divorce or legal separation,
- enrollment in Medicare, or
- the end of a child's dependency under a parent's health plan

Title IV – Application & Enforcement of Group Health Plan Requirements

Consolidated Omnibus Budget Reconciliation Act

- Mandates an insurance program which gives some employees the ability to continue health insurance coverage after leaving employment.

- Maximum period of COBRA coverage is 18 months.
- An employer is permitted to charge qualified beneficiaries 102 percent of the applicable premium for COBRA coverage.
- A tax is imposed on the failure of a group health plan to satisfy the COBRA rules.

COBRA – Example

Example

A plan has a coverage rule that states a surviving spouse's benefits end at the end of the month following the month in which a covered employee or retiree dies. In the retiree context, an employer that does not know of a death not only has to deal with potential COBRA violations, but it must address the fact that it could be providing coverage to individuals who are not entitled to it based on the plan rule. An audit may identify surviving spouses who had continued to remain covered under the plan after the end of the month following the retiree's death.

Title V – Revenue Offsets

- Loans against company-owned life insurance policies
  - Corporate-owned life insurance (COLI) is commonly used to fund non-qualified deferred compensation (NQDC) plans
- Treatment of individuals who lose U.S. citizenship
- How financial institutions allocate interest

What Are The Penalties If You Do Not Comply?

- Civil Penalties under HIPAA
  - Maximum fine of $25,000 per violation
- Criminal Penalties under HIPAA
  - Maximum of 10 years in jail and/or a $250,000 fine for serious offenses
- Organization Actions
  - Employee disciplinary actions including suspension or termination for violations of the organizations policies and procedures

HITECH Act Overview

- The HITECH Act was passed as a part of the American Recovery and Reinvestment Act of 2009 (ARRA), which was signed into law **February 17, 2009. HITECH extends the HIPAA law.**

- **HITECH** includes enhanced privacy and security requirements for covered entities, business associates**, and personal health record (PHR)** vendors. The provisions include:
  - Increased HIPAA violation penalties and refined enforcement provisions
  - Extended HIPAA regulatory liability to business associates
  - A Federal data breach notification rule regarding PHI

- HITECH went into effect in **February 2010**

Breach Notification Requirements

- Notification is required to the affected individuals, the government and in certain cases the media [if the breach involves more than 500 people] in the event of a breach of “Unsecured Protected Health Information”.
- These breach requirements are applicable to both Covered Entities [CE] and their Business Associates.
- If the Covered Entities Business Associate has a breach, they must report it within 60 days.

For validation and assessment of HIPAA scope applicability, Infinite account teams should contact the HIPAA Program Officer:

By email to Compliance-Team@infinite.com

Consequences of not complying with HITECH

- Penalties for non-compliance, ranging from fines of $100 to $50,000 per violation, capped at $25,000 to $1.5 million per violation of the same standard.
- Criminal penalties of 1 to 10 years in jail for gross negligence
- HITECH also created new methods for enforcement, allowing state attorney generals to enforce HIPAA regulations

Thank You.

© 2015 Infinite Computer Solutions . All Rights Reserved