HIPAA Compliance; an Executive Overview

This class provides an overview of the current HIPAA 45 C.F.R. regulations that healthcare agencies need to follow to achieve compliance.

Training content accurate as of 1/28/2016 and will not reflect any regulation changes that are published after that date.

Copyright © by Xpio Health. All rights reserved.
Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996

Under Title II
- Administrative Simplification
- Preventing Healthcare Fraud and Abuse
- Medical Liability Reform
- Electronic Data Exchange; i.e.: 837, 835
- Security
  - Administrative, Physical and Technical Safeguards
- Privacy
• Health Information Technology for Economic and Clinical Health Act
• Included in the American Recovery and Reinvestment Act (ARRA) of 2009
• Contains incentives related to healthcare technology in general and specific incentives designed to accelerate the adoption of electronic health records
• Meaningful Use
• Added “teeth” to HIPAA
• Wall of Shame: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
• Notice of Privacy Policies (NPP)
• Business Associates (BA) Agreements
  ◦ BA now just as responsible and accountable
• Policies and Procedures
• Training Requirements
• Audits
• Mandated Breach Notification
• Expanded Privacy and Patient Rights
• Expanded and Mandated Security
• Enforcements and enhanced monetary penalties
• Office of Civil Rights (OCR) enforcement authority
• State Attorneys General enforcement
**Covered Entity**

A Covered Entity is a healthcare delivery option that includes doctors, clinics, hospitals, dentists, nursing homes and pharmacies that transmit data, health plan and healthcare clearinghouses.

**Business Associate**

A Business Associate is any person or organization that functions on behalf of a covered entity that involves use or disclosure of identifiable health information. Examples include billing and coding vendors.
Security Roles are established to provide governance of the HIPAA program. Under the HIPAA Security Rule 45 C.F.R. 164.308 (a)(2), overall responsibility is required to reside in a single person with other roles assigned as needed. A single person may be assigned to more than one role:

- Security Compliance Officer
- Privacy Officer
- Workforce Security Manager
- IT Security Manager
- Incident/Breach Manager
- Physical Security Manager
What is Protected Health Information (PHI)?

- Name
- Address
- Dates directly related to patient
- Telephone number
- Fax Number
- Email addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary Number

- Account Number
- Certification/License Number
- Any vehicle or device serial number
- Web URL, IP address
- Finger or voice prints
- Photographic images
- Any other unique number, characteristic or code
- Age greater than 89
• What information is Protected?

All Medical Records and Other Individually Identifiable Health Information (PHI) Used or Disclosed by a Covered Entity in any Form; Electronic, on Paper or Orally

• What is Included?

Individually Identifiable Information that was provided by the client, created by you, created by another and forwarded to you and forwarded to you for payment, treatment or healthcare operations.
A CE is permitted, but not required, to use and disclose PHI without an authorization, for the following purposes:

- To the individual
- Treatment, Payment and Health Care Operations (TPO)
- Opportunity to Agree or Object to a facility directory
- Incident to an otherwise permitted use
- Limited Data Set for purposes of research, public health or health care operations
A Business Associate may use or disclose PHI only as permitted or required by its BA contract or other arrangement required by law.

A BA is required to disclose PHI when the Secretary requires it and to the CE, individual or individual’s designee, as necessary, to satisfy the CE’s obligations.
**Patient Rights under HIPAA**

- To see their medical record
- Obtain a copy of their medical record
- Request amendments to their medical record
- Request disclosure restrictions
  - Private Pay
  - Certain other disclosures, including research and marketing
- To authorize disclosures
- To receive a Notice of Privacy Practices
- To have an accounting of disclosures (not TPO)
- Timely notification of any breaches
- Secure Communications
- Confidential communications when requested
California Laws that protect Medical Information
- The Confidentiality of Medical Information Act (CMIA)
- The Information Practices Act (IPA)
- The Patient Access to Health Records Act (PAHRA)
- The Insurance Information and Privacy Protection Act (IPPA)
| HIPAA permits Covered Entities to use or disclose PHI to the extent such use or disclosure is required by law and complies with the law. Covered Entities must comply with specific disclosures (report abuse, etc) | State law; The CMIA permits disclosure of medical information where such disclosure is compelled by a competent legal authority or process as specified (Civil Code Section 56.10 (b)) | Analysis: HIPAA permits California providers to continue to comply with most required disclosures under CMIA. |

**Federal and State Notification Laws-CHA Analysis**
• Please refer to the entire CHA paper for additional detailed information on disclosure analysis CMIA compared to HIPAA
• As we already mentioned, the most stringent law takes precedent
• Find the Preemption Analysis Chart; Patients Covered by CMIA in the resources link in the upper right corner of the slide
Now, the Rules
According to the Department of Health and Human Services, the HIPAA Security Rule outlines national standards designed to protect individual’s electronic PHI.

The HIPAA Privacy Rule set a national standard for the protection of certain health information that addresses the use and disclosure of PHI and standards for privacy rights for patients to understand and control how their health information is used.
In May 2005, the Security Rule was implemented. It covers:

- Access Control
- Anti-Virus, Anti-Malware
- Strong Passwords
- Remote Access
- Locks
- Technical Security
- Back up and Recovery
- Risk Analysis Requirement
The Code of the Federal Register (CFR) is the codification of the general and permanent rules published in the Federal Register.

Title 45, Subtitle A, Subchapter C, Part 164 covers Security and Privacy.
• Also included:
  ◦ Risk Analysis
  ◦ Risk Management
  ◦ Sanction Policy
  ◦ IS Activity Review
  ◦ Response and Reporting
  ◦ Data Back up/Business Continuity Plan
  ◦ Media Disposal/Re-use
  ◦ Unique User ID
  ◦ Business Associate Agreements
  ◦ Written Policies and Procedures
The goal of the HIPAA Privacy Rule is to properly protect individual’s health information and to use PHI appropriately while protecting the privacy of people who seek care and healing.
Privacy covers both paper and electronic data.
In December 2012, Leon Rodriguez, then-director of the US Department of Health and Human Services’ Office of Civil Rights (OCR) warned “We’ve now moved into an area of more assertive enforcement.”
• Breach Definition

An impermissible use or disclosure under the Privacy Rule of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

Breaches of more than 500 patient records must be reported to the news media.
Key Findings:

- May sees a 62% reduction in reported data breaches compared to April.
- However, those breaches affected 72% more people than in April.
- The number of breach victims reported for May, 2015 is already 59% higher than May, 2014.
- 110 healthcare data breaches have been reported to the OCR so far in 2015.
- Year to date figures show a fall in reported data breaches of 16% compared to 2014.
- Hackers have stolen 92,920,060 records so far in 2015. This time last year the figure was just 462,670 records.
- 42% fall in reported thefts for the year and an 87% reduction in the number of breach victims.
- Only 2 Business Associates have reported data breaches in 2015, a fall of 95% year on year.

Key Findings
Following a breach of unsecured PHI, Covered Entities must provide notification of the breach to the affected individual, the Secretary, and in certain circumstances, to the media.

Business Associates must notify the Covered Entity of a breach.

Provided without unreasonable delay, no later than 60 days following the discovery of the breach.

- CA requires a 15 day maximum

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

**Reporting Requirements**
• Criminal Penalties-Covered Entities and specified individuals whom “knowingly” obtain or disclose PHI can face up to $50,000 fine, as well as up to one year in prison.
• Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine and up to five years in prison
• Offenses committed with the intent to sell, transfer to use info for personal gain has fines up to $250,000 and up to 10 years in prison
<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
42 CFR Part 2

Promote Access to Treatment

Core Values of 42 CFR, Part 2

Confidentiality

Reduce Stigma

Nurture the Doctor-Patient Relationship
42 CFR Part 2 (commonly referred to as "Part 2") are the federal regulations governing the confidentiality of drug and alcohol abuse treatment and prevention records.

- Privacy protections afforded to alcohol and drug abuse patient records
- Motivated by the understanding that stigma and fear of prosecution might dissuade persons from seeking treatment

42 C.F.R., Part 2
• 42 CFR Part 2 applies to any individual or entity that is federally assisted and provides alcohol or drug abuse treatment or referral for treatment (42 CFR § 2.11)
• Consider funding, treatment provided and clinical licenses that are at the federal level (DEA license)
• Restrict the disclosure and use of alcohol and drug client records
• Any information disclosed by a covered program that “would identify a patient as an alcohol or drug abuser” (42 CFR §2.12(a) (1)
• With limited exceptions, 42 CFR Part 2 requires client consent for disclosures of PHI even for the purposes of TPO. Consent must be in writing
Includes the electronic codes of federal regulations

Introduction, General Provisions, Disclosures with Patient Consent, Disclosures without Patient Consent, Court Orders Authorizing Disclosure and Use

http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2
The primary way in which patient substance abuse information may be disclosed is with a patient’s written consent. Substance abuse programs and providers must give patients a written summary of the federal laws and regulations that protect the confidentiality of patient substance abuse records and a description of the circumstances when the patient’s information may be disclosed without his/her consent.
For all other disclosures, consent must be obtained using a written consent form. A single consent form may authorize disclosure to multiple parties or for multiple purposes.

Consent forms must contain specific elements.
Exceptions—Always work with Privacy Officers

- Program Communications
- To communicate with Qualified Service Organizations (QSO)
  - Similar to other covered entities or business associates
- Medical Emergencies
- Response to a crime against program personnel or on program premises

- Research activities (approved by IRB)
- Audit and Evaluation
- Report suspected child abuse or neglect
- Circumstances involving certain minors or incompetent patients
- Response to a valid court order
- Cause of death
• Substance use programs must comply with both HIPAA 45 CFR and 42 CFR Part 2
• If there is a conflict, the more stringent rule applies
• Add link to comparison table**
• You begin to see that addiction treatment providers fall under the more stringent laws of 42 CFR, Part 2, in most cases.
• However, there are requirements of HIPAA that must be put into place on specific forms that previous laws didn’t address or mandate.
The Substance Abuse and Mental Health Services Administration (SAMHSA) provides great information and support on 42 CFR Part 2.
Spearheading efforts to change 42 CFR Part 2 to accommodate sharing info in EHRs/HIEs.
http://www.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs
- Must be current and reference 45 CFR for both privacy and security
- Agency must have an interconnected set of policies, plans, procedures and security roles assigned to have the end result be a secure, compliant and auditable environment
Types of Policies

- Acceptable Use Policy
- Business Associate Policy
- Incident Response Policy
- Malicious Software Policy
- PHI Protection Policy
- Perimeter, Remote Access and Wireless Policy
- Privacy Protection Policy
- Security Management Policy
- Violations Sanctions Policy
- Workforce Security Policy

- Access Control Policy
- Contingency Planning Policy
- Information System Monitoring Policy
- Mobile Device and Media Security Policy
- Password Policy
- Physical Security Policy
- Risk Management Policy
- Security Roles Policy
- Vulnerability Assessment Policy
- Workforce Training Policy
Types of Procedures

- Access Control SOP
- Backup and Restore SOP
- Encryption SOP
- Other Device Configuration SOP
- Security Violations SOP
- Training Content SOP
- Training Plan SOP
- Wireless Configuration SOP
- Workstation Configuration SOP
- Application Configuration SOP
- Decommission SOP
- Mobile Configuration SOP
- PHI Inventory SOP
- Server Configuration SOP
- Training Documentation SOP
- Vulnerability Assessment SOP
- Workforce Security SOP
Types of Plans

Contingency Plan
Physical Security Plan

Incident Response Plan
Agencies must ensure all employees and temporary users given access to sensitive information have the training necessary to securely operate hardware and software to protect PHI.

A training strategy, training plan and training materials are required to meet compliance.
Next Steps for Agencies:

- Establish a HIPAA Compliance Team that covers all Security Roles
- Review the current Policies and Procedures against the 45 C.F.R sections 164.305-316, 506 and confirm policies are updated
- Confirm control over all PHI in the agency; both paper and electronic
- Train Staff at hire, annually and have subsequent trainings/reminders throughout the year
- Create a culture of Compliance
Next Steps

- Review your Business Continuity, Physical Security and Incident Response plans for current processes and TEST
- Complete your annual reviews and document
Audits

- Healthcare agencies must comply with Office of Inspector General (OIG) audits to confirm they are protecting health information.
- Audits cover the security and privacy risk assessments, security plan, org charts, network diagrams, portals, P&Ps, system inventory, tools for network scans, logs, user access and contractors (BA)
Take your Exam

- Go to www.xpiohealth.org/cibhs and register to take the HIPAA for Executive Leadership exam. Use the coupon codes as described in the “how to register” document.
- Print out your certification of completion and feel proud of your success!
- Remember to share your HIPAA knowledge with others in your agency, create that culture of compliance.