HIPAA AND YOU
2017

GERALD E MELTZER, MD MSHA
ALLISON SHUREN, JD, MSN
Financial Disclosure

• Gerald Meltzer is a consultant for iMedicWare

• Allison Shuren co-chairs the Life Sciences and Healthcare Regulatory Practice at Arnold and Porter Kaye Scholer, LLP

• Neither of the presenters have any financial interest in the subject being presented
Course Objectives

• Learn key elements of HIPAA
• Learn how to build a culture of compliance
• Learn how to prevent loss or misuse of PHI
• Learn when it is permissible to share patient data
• Present real work examples
QUESTIONS

• HIPAA Training Last 12 Months?
• Ransomware Attack?
• Last Security Risk Analysis?
• Do you Encrypt Email?
• Encryption/AntiVirus on Mobile Devices?
• Fax Follow-up?
• BAA Audit?
• Privacy Officer?
WHY HIPAA?

• Protect patient’s rights
• These rights (to privacy and confidentiality) are considered fundamental civil rights
• Because of this, HIPAA is administered by the Office of Civil Rights (OCR)
WHAT RIGHTS?

• Protection of privacy and security of your health information
• Access to your health information
• Request correction of your health information
• Restrict certain disclosures of your health information
• Notification if the privacy or security of your information is compromised
• Information about how your health information will be used or disclosed
HIPAA AT A GLANCE

• HIPAA stands for Health Insurance Portability and Accountability Act
  • History
    • 1996 Kennedy and HIPAA Part 1
    • 2003 HIPAA Final Rule Part 2
    • 2006 Enforcement Rule
    • 2009 ARRA and HiTech
    • 2013 HIPAA HiTech Omnibus Rule
    • 2016 BAA/Cloud/Mobile

• Privacy rule
• Security Rule
• Breach Notification Rule
Privacy Rule

- Established national standards for protection of all forms of health information created by covered entities including health care providers
- Set limits on all uses and disclosures of this information
- Gave patients rights over their health plan information
Security Rule

• Established national standards to protect electronic personal health information (ePHI) created, received, used or maintained by covered entities
• Outlines administrative, technical, physical procedures to ensure the confidentiality, integrity and availability of ePHI
HITECH OMNIBUS RULE 2013

• Health Information Technology for Economic and Clinical Health Act
  • Update to HIPAA – recognizes technology must be appropriate to promote security of electronic records and sensitive information

• BREACH NOTIFICATION RULE
  • Breach is presumed unless it can be demonstrated low probability of PHI compromise
  • Less than 500 records – report annually
  • Over 500 records – report within 60 days
  • Business Associates must also provide notice

• Other
  • Business Associates agreements updated and expanded
  • Strengthen Privacy Protections
  • Increased Penalties
HIPAA VIOLATIONS

• Since 2003 – 123,065 HIPAA violations reported
• Since 2009 – 1,900 violations involving 175 million patient records
• Average Settlement Cost $800,000
• September 2012 Mass Eye and Ear – stolen laptop 1.5M
• May 2014 Columbia Presbyterian – unauthorized access 4.8M
• All HIPAA breaches of more than 500 patients are posted on the web on the WALL OF SHAME
<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memorial Hospital Clinic South</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>842</td>
<td>4/26/2017</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Network Server</td>
</tr>
<tr>
<td>Memorial Hospital Clinic West</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>521</td>
<td>4/26/2017</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Network Server</td>
</tr>
<tr>
<td>Atlantic Digestive Specialists</td>
<td>NH</td>
<td>Healthcare Provider</td>
<td>2081</td>
<td>4/21/2017</td>
<td>Ransomware</td>
<td>Network Server</td>
</tr>
<tr>
<td>Iowa Veterans Home</td>
<td>IA</td>
<td>Healthcare Provider</td>
<td>2969</td>
<td>4/21/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email Phishing</td>
</tr>
<tr>
<td>Lifespan Corporation</td>
<td>RI</td>
<td>Healthcare Provider</td>
<td>20431</td>
<td>4/21/2017</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Behavioral Health Center</td>
<td>ME</td>
<td>Healthcare Provider</td>
<td>4229</td>
<td>4/21/2017</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Valley Women’s Health, S.C.</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>5155</td>
<td>4/19/2017</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Network Server</td>
</tr>
<tr>
<td>Bioreference Laboratories, Inc.</td>
<td>NJ</td>
<td>Healthcare Provider</td>
<td>1772</td>
<td>4/14/2017</td>
<td>Improper Disposal</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Western Health Screening</td>
<td>MT</td>
<td>Business Associate</td>
<td>15326</td>
<td>4/14/2017</td>
<td>Theft</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>MVP Health Care, Inc.</td>
<td>NY</td>
<td>Health Plan</td>
<td>951</td>
<td>4/14/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Area Agency of Aging 1-B</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>1741</td>
<td>4/13/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>Eyecare Services Partners Management, LLC</td>
<td>TX</td>
<td>Business Associate</td>
<td>9129</td>
<td>4/12/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Amedsys West Virginia, LLC</td>
<td>WV</td>
<td>Healthcare Provider</td>
<td>611</td>
<td>4/11/2017</td>
<td>Improper Disposal</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>Cardiology Center of Acadiana</td>
<td>LA</td>
<td>Healthcare Provider</td>
<td>9681</td>
<td>4/7/2017</td>
<td>Hacking/IT Incident/Ransomware</td>
<td>Network Server</td>
</tr>
<tr>
<td>Carson Valley Medical Center</td>
<td>NV</td>
<td>Healthcare Provider</td>
<td>11368</td>
<td>4/4/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>University of Oklahoma, OU Physicians</td>
<td>OK</td>
<td>Healthcare Provider</td>
<td>1637</td>
<td>4/4/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>Ashland Women’s Health</td>
<td>KY</td>
<td>Healthcare Provider</td>
<td>19727</td>
<td>4/4/2017</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Memorial Healthcare</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>685</td>
<td>4/3/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Apex EDI, Inc.</td>
<td>UT</td>
<td>Business Associate</td>
<td>1132</td>
<td>3/31/2017</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Skin Cancer Specialists, P.C.</td>
<td>GA</td>
<td>Healthcare Provider</td>
<td>3365</td>
<td>3/31/2017</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Women’s Care of Somerset</td>
<td>KY</td>
<td>Healthcare Provider</td>
<td>1806</td>
<td>3/31/2017</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>ABCD Pediatrics, P.A.</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>55447</td>
<td>3/26/2017</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Lane Community College Health Clinic</td>
<td>OR</td>
<td>Healthcare Provider</td>
<td>1911</td>
<td>3/25/2017</td>
<td>Hacking/IT Incident</td>
<td>Laptop</td>
</tr>
<tr>
<td>Washington University School of Medicine</td>
<td>MO</td>
<td>Healthcare Provider</td>
<td>80270</td>
<td>3/25/2017</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
</tbody>
</table>
HIPPA COVERS

• Entities who collect or have access to PERSONAL HEALTH INFORMATION INCLUDING
  • Medical providers, hospitals, or health plans that conduct certain electronic transactions related to **billing**
    • Billing health plans for treatment
    • Validating insurance
    • Paying for treatment
  • Business Associates and their subcontractors
SIMPLY PUT HIPAA COVERS

• ALL paper and electronic identifiable patient data
• Created OR Received OR Accessed BY
• A HIPAA Covered Entity OR A Business Associate
• This can include
  • A note written on a napkin OR
  • A formal medical record OR
  • A photograph OR
  • A voice message
What is PROTECTED HEALTH INFORMATION?

• INFORMATION ABOUT PATIENT’S DIAGNOSIS OR TREATMENT OR PAYMENT
  • PAST
  • PRESENT
  • FUTURE

• THAT IS IDENTIFIABLE

• HIPAA defines 18 separate identifiers
  • Name, Address, Dates, Phone #, Fax #, Email, SSN, MRN, Account #, Web URL
  • Insurance Info, Vehicle Info, License, IP Address, Fingerprint, Photo Image, Ohter
ePHI INCLUDES

• Information stored in medical records PLUS PHI contained in:
  • Email messages and attachments
  • Faxes
  • Word processing documents
  • Spreadsheets
  • Reports
  • Scanned Documents
  • Medical Images/Photographs
  • Voice Messages
WHAT IS A BUSINESS ASSOCIATE

• Person or an entity (other than member of your office staff)
• Performs services which involve
  • Access or Use or Disclosure of PHI
• Activities include
  • Claims processing
  • Quality Assurance
  • Utilization Review
  • Billing
WHAT IS A BUSINESS ASSOCIATE

• BA services can include
  • Legal
  • Accounting
  • Consulting
  • Information Technology Management

• Examples include
  • Health Information Exchanges
  • E Prescribing gateways
  • Subcontractor to a BA that creates, receives, maintains or transmits PHI on behalf of a BA
WHAT INFORMATION CAN I RELEASE?

• Information needed for treatment, payment and health care operations

• IF YOU HAVE PERMISSION - you can release information to family or friends involved in patients care OR to other persons that the patient identifies

• In emergency situation, if provider determines it is in the best interest of the patient

• Information Public Health and Safety
  • Immunization records
  • Risk of communicable disease
HIPAA VIOLATIONS

• Hacking – largest number of records stolen
• Lost unencrypted media and devices largest number of incidents
• Failure to obtain BAA
• Average Data Breach cost $401 per record

• This applies to both the CE AND the BAA (and their subcontractors)
TRUE OR FALSE?

• We only have to protect our EHR
• All our protected data is stored on our servers
• Our EHR system is in the cloud so we don’t have to worry about cybersecurity in our office or on our computers
• We have bought a HIPAA notebook so we are now HIPAA compliant
<table>
<thead>
<tr>
<th>Myth</th>
<th>Fact</th>
</tr>
</thead>
<tbody>
<tr>
<td>The security risk analysis is optional for small providers.</td>
<td>False. All providers who are &quot;covered entities&quot; under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.</td>
</tr>
<tr>
<td>Simply installing a certified EHR fulfills the security risk analysis MU requirement.</td>
<td>False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.</td>
</tr>
<tr>
<td>My EHR vendor took care of everything I need to do about privacy and security.</td>
<td>False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.</td>
</tr>
<tr>
<td>I have to outsource the security risk analysis.</td>
<td>False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.</td>
</tr>
<tr>
<td>A checklist will suffice for the risk analysis requirement.</td>
<td>False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.</td>
</tr>
<tr>
<td>Statement</td>
<td>Correction</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>There is a specific risk analysis method that I must follow.</td>
<td>False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.</td>
</tr>
<tr>
<td>My security risk analysis only needs to look at my EHR.</td>
<td>False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.</td>
</tr>
<tr>
<td>I only need to do a risk analysis once.</td>
<td>False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see the Reassessing Your Security Practice in a Health IT Environment.</td>
</tr>
<tr>
<td>Before I attest for an EHR incentive program, I must fully mitigate all risks.</td>
<td>False. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.</td>
</tr>
<tr>
<td>Each year, I’ll have to completely redo my security risk analysis.</td>
<td>False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP’s year of participation in the program.</td>
</tr>
</tbody>
</table>
Guide to Privacy and Security of Health Information

The complete document (47 pages) may be downloaded from:

Version 1.1 02/21 12

The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in Health IT
www.HealthIT.gov
Ransomware and HIPAA

• Security Risk Assessment
• Mitigate Risk (malware)
• Detection (audit)
• Recovery Procedures in place?
• If Ransomware detected
  • Security Risk Assessment/Analysis/Breach?
  • If data encrypted and no user interaction – no breach
  • If data encrypted but in use – then breach has occurred
What about Mobile Devices?

- Mobile Devices
  - Laptops
  - Smart Phones/Tablets
  - Cameras

- Storage Media
  - CD’s/DVD’s
  - USB Drives
  - Memory Cards, Disks, etc.

- Do not store PHI on Mobile Devices or External Storage Media unless it is absolutely necessary.

- If it is necessary then the device MUST be encrypted and password protected where technically feasible.
So what should I do?
CHECK LIST
ADMINISTRATIVE SAFEGUARDS

• Designate Security/Privacy Officer
• Workforce Training
• Security Risk Analysis
SECURITY RISK ANALYSIS – TRAINING

• Written manuals not enough
• Keep Records of all training - certificates
• ALL employees must be trained
  • Retrain OLD employees annually
  • New employees – train within 30 days
  • If the law changes – employees must be retrained

• Health Care Compliance Pros – www.hcp.md
SECURITY RISK ASSESSMENT TOOL

- Downloadable SRA TOOL
- Search for Security Risk Analysis Tool
- Available for Windows, Mac and iPAD
- 156 YES/NO Questions
- Instruction Manual

- See https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
§164.308(a)(1)(I) - Standard
Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

Yes ☐ No ☐ Flag ☐

Current Activities
Eye Care Professionals has developed, documented and provided to all of its employees a risk assessment policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also outline procedures to facilitate its implementation and associated risk assessment controls.

With respect to a threat/vulnerability affecting your ePHI:

Likelihood: ○ Low ☐ Medium ☐ High
Impact: ○ Low ☐ Medium ☐ High

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Electronic storage media includes...
CHECK LIST
PHYSICAL SAFEGUARDS

• Office Access
• Building Alarms
• Lock Office
• Portable Devices - LoJack
CHECK LIST
TECHNICAL SAFEGUARDS

• Password Control
• Routine Audits
• Anti-hacking and anti-malware software installed and updated
• Contingency Plans
• Encrypt Your Data
  • Office computers
  • Mobile Devices
  • Storage Data
CHECK LIST
ORGANIZATIONAL STANDARDS

• Business Associate Agreements
  • Regularly Reviewed
  • Updated as necessary
  • Confirm business associates are trained and have contingency plans
• Review all policies and procedures annually
• Security Team conducts monthly review of user activities
• Ongoing Training annually
CYBERSECURITY INSURANCE

• COVERS
  • Legal and fines for violation HIPAA privacy and security regulations
  • Network Asset Protection – digital asset loss, theft
  • Cyberextortion – threat to release confidential information or corrupt computer system
    • will pay to terminate threat
    • Will pay to restore system
  • Security or privacy wrongful act
    • Regulatory fines
    • Legal expense
  • In case of security breach – will pay for PR consultant to help mitigate damage and will pay for credit file monitoring
Case #1

• Who has ePHI on you laptop?
• Is your laptop secure?
• Who has ever left your laptop in your car?
• Who has ever had a laptop stolen? From where? Your car?
• What do you think the penalty might be for a stolen laptop?

$2.5 Million
CardioNet

- Provider of remote cardiac monitoring services
- Impermissible disclosure of unsecured ePHI through laptop stolen from employee’s car
- Self-reported to OCR twice, 1 month apart
- Findings
  - Insufficient security risk analysis and risk mgm processes
  - No P/P for security
  - No P/P for safeguarding ePHI
  - Failure to take immediate action to correct disclosure
CardioNet

- Penalty: $2.5 million
- Corrective Action Plan
  - Comprehensive security risk assessment to be submitted to OCR
  - Annual review thereafter
  - Develop risk management plan
  - Implement secure device and media controls
  - Training
  - Annual report to OCR
Case #2

- Physician practice
- Findings
  - Failed to obtain a Business Associate agreement with medical record storage service
  - 17,300 medical records released to storage company
- Penalty: $750,000
- Corrective Action Plan
  - Complete P/P
  - Conduct training on P/P and obtain employee confirmation
  - Annual update of P/Ps
  - List of reportable events
  - Annual report of BAs
Case #3

• Hospital

• Findings
  • Failure to follow minimum necessary requirement
  • A hospital employee left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. Patients had instructed that messages were to be left on her work number, not home.

• Corrective Action Plan
  • Hospital required to develop and implement new procedures to address the issue of minimum necessary information in telephone message content.
    • Script of what information may be provided in telephone messages.
    • Employees also were trained to review registration information for patient contact directives regarding leaving messages.
  • Train employees on new P/Ps.
  • Annual training required and documentation provided to OCR.
Case #4

• Physician Practice

• Findings
  • A staff member of a medical practice discussed HIV testing procedures with a patient in the waiting room, thereby disclosing PHI to several other individuals.
  • Computer screens displaying patient information were easily visible to patients.

• Corrective Action Plan
  • Develop and implement policies and procedures regarding appropriate administrative and physical safeguards related to the communication of PHI.
  • Train all staff on the newly developed policies and procedures. In addition.
  • Reposition its computer monitors to prevent patients from viewing information on the screens and install computer monitor privacy screens.
Case #5

• Physician Practice

• Findings:
  • A patient alleged that a covered entity failed to provide him access to his medical records.
  • After OCR notified the entity of the allegation, the entity released the complainant’s medical records but also billed him $100.00 for a “records review fee” as well as an administrative fee.
  • The Privacy Rule permits the imposition of a reasonable cost-based fee that includes only the cost of copying and postage and preparing an explanation or summary if agreed to by the individual.

• Resolution: Covered entity refunded the $100.00 “records review fee.”
Case #6

• ASC

• Findings
  • ASC disclosed a patient's (PHI) to a research entity for recruitment purposes without the patient's authorization or an Institutional Review Board (IRB) or privacy-board-approved waiver of authorization.
  • ASC reportedly believed that such disclosures were permitted by the Privacy Rule.

• Corrective Action Plan
  • OCR provided technical assistance regarding the requirement that covered entities seeking to disclose PHI for research recruitment purposes must obtain either a valid patient authorization or an IRB or privacy-board-approved alteration to or waiver of authorization.
  • ASC required revise its written policies and procedures regarding disclosures of PHI for research recruitment purposes to require valid written authorizations.
  • Retrain its entire staff on the new policies and procedures.
  • Utilize a log the disclosure of the patient's PHI for accounting purposes.
  • Send the patient a letter apologizing for the impermissible disclosure.
Cyber Liability Insurance

• Many practices are purchasing cyber liability insurance that protects against data breaches. Costs often covered include:
  • Contacting customers after a breach of private information;
  • Hiring information technology forensic specialists to investigate a breach and figure out where the leak occurred;
  • Deploying public relations/marketing professionals to handle the community messaging required by certain breaches;
  • Providing credit monitoring for patients whose records were exposed; and
  • HIPAA fines.

• Not all cyber liability policies cover HIPAA fines, and some may limit coverage based on the nature of the HIPAA violation. For instance, a $1 million policy may allow $200,000 to be spent on HIPAA fines.
TAKE HOME TO DOS

• Conduct a HIPAA Risk Assessment
• Designate and Train Privacy Officer
• Update Policies and Procedures
• Train Staff
• Update Business Associate Agreements
• Document All Access to PHI
• Correct Deficiencies
• The time to learn HIPAA is BEFORE a breach