MentorHealth

Live Webinar

on

New HIPAA Rules – Meeting Requirements for New Patient Rights and New Restrictions on Disclosures

Presented by ***Jim Sheldon-Dean***

Tuesday, June 2nd, 2015 10:00 AM PDT | 01:00 PM EDT

Agenda

- Discussion of changes to the HIPAA rules and required changes to your HIPAA policies and procedures – new rights for individuals and new obligations, including:
  - New rights for electronic copies of electronic records
  - New right to request certain restrictions that MUST be agreed to
  - Changes in how to determine whether a breach is reportable or not
  - Changes in Marketing and Fundraising practices
  - New rights of access to Laboratory test results
- Updating your Notice of Privacy Practices, Policies, and Training
- Expansion of HIPAA regulations to Business Associates
- Proposed changes to Accounting of Disclosures not finalized yet
- New guidance on mental health information
- Discuss enforcement, penalties, and auditing

MentorHealth

My Background

- Disclaimer: I am an engineer and not a lawyer. This is not legal advice – I am only providing information and resources
- BSCE (Civil Engineering) from UVM, MST (Transportation) from MIT
- 33 years in consulting, information systems, software development, and information privacy and security
- Process, problem-solving oriented
- 8 years as Vermont EMT, crew chief
- 15 years specializing in HIPAA and health information privacy and security regulatory compliance
- See www.lewiscreeksystems.com for more details, resources, information privacy and security compliance news, etc.

MentorHealth

The Long Path of HITECH

- Health Information Technology for Economic and Clinical Health Act (HITECH Act) – Title XIII, Subtitle D-Privacy (all the sections 134xx) of the American Recovery and Reinvestment Act of 2009
- Most of the proposed rules finalized in the big HIPAA Omnibus Update, enforceable September 23, 2013
- Omnibus Update Rule, with Preamble, available at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- New Combined Rules published by HHS OCR, available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

MentorHealth

HIPAA Privacy and Security Rules

- Privacy Rule
  - 45 CFR § 164.5xx
  - Enforceable since 2003
  - Establishes Rights of Individuals
  - Controls on Uses and Disclosures
  - Access of PHI is a hot button issue for HHS
  - Several changes under the new rules
- Security Rule
  - 45 CFR § 164.3xx
  - Enforceable since 2005; Applies to all electronic PHI
  - Flexible, customizable approach to health information security
  - Uses Risk Analysis to identify and plan the mitigation of security risks
  - Only change under the new rules is to extend to Business Associates

MentorHealth

HIPAA Breach Notification Rule

- CFR 45 Part 164 Subpart D; 45 CFR §164.4xx
- Enforceable since February 2010, Final Rule now in effect, with new changes in how to determine if a breach must be reported
- Works with Privacy and Security Rules
- Requires reporting of all PHI breaches to HHS and individuals; breaches affecting 500 or more individuals must be reported to individuals, HHS, and the Press simultaneously
- Provides great examples of what not to do; HHS "Wall of Shame": https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

MentorHealth

What's New in HIPAA?

- New individual rights of access
- New individual rights to request restrictions
- Change in the way to determine if a breach must be reported
- New restrictions on disclosures for marketing, sale of PHI; changes to rules for use of PHI for fundraising
- New restrictions on use of genetic information by health plans (must be noted in Notice of Privacy Practices for the plans)
- New allowance for access to Laboratory information
- PHI not protected > 50 years after individual's death
- Notices of Privacy Practices must be updated to reflect new individual rights and privacy practices
- Expansion of rules to Business Associates

MentorHealth

PHI, Uses, and Disclosures

- Protected Health Information (**PHI**): Individually identifiable information about health, health care, or payment for healthcare services
- **Disclosure**: the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information
- As distinct from **Use**: the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information

MentorHealth

More Definitions: DRS, TPO

- Designated Record Set (DRS)
  - The medical records and billing records about individuals maintained by or for a covered health care provider;
  - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  - Used, in whole or in part, by or for the covered entity to make decisions about individuals.
- Treatment, Payment, and Healthcare Operations (TPO)
  - Relating to provision, coordination, and management of healthcare services
  - Reviews, determinations, billing, collection
  - Case management, workforce evaluation, peer review, outcomes analysis, etc. related to YOUR operations
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html

MentorHealth

Accounting of Disclosures

- Individual has right to an accounting of all disclosures of health information in last six years
- Except for disclosures:
  - For Treatment, Payment, and Healthcare Operations
  - To the individual; under authorization; associated with disclosures under §164.502; for facility directories; for national security; law enforcement; limited data set…
- Proposed Rule to implement changes under HITECH Act NOT included in the Omnibus HIPAA Update
- New recommendations for a staged implementation, limited to available technology, a much better proposal! http://www.healthit.gov/FACAS/sites/faca/files/HITPC_PSTT_Accounting%20of%20Disclosures_FINAL_12042013.pdf

MentorHealth

Restriction of Disclosures

- Must have a process for individuals to request restrictions on use and disclosure
  - Need not honor requests
  - Do what you reasonably can
- New: Individual may request no information shared with insurer if paid in full out of pocket
  - MUST honor the request!

MentorHealth

Impact of Restriction of Disclosures to Insurers

- Must have a policy/procedure/process
- Required in your EHR to meet the law
- Can you flag such encounters?
  - Create non-billable procedure codes for self-pay
  - What about pass-through effects?
  - Issues with aggregated data
  - What about contracts with insurers?
- May need to update BA Agreements
- Will need to update the Notice of Privacy Practices
- Not easy to comply with – does your EHR have this?

MentorHealth

Marketing Changes

- Marketing is still marketing and still requires an authorization
- Treatment and Healthcare Operations are not marketing, but…
- Authorizations are now required for all treatment and healthcare operations where the Covered Entity receives financial remuneration from a third party whose product or service is being marketed
- New guidance available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/marketingrefillreminder.html
- Exemptions:
  - Face to Face communication
  - Refill reminders or other info about a drug or biologic that is currently prescribed but not exempt if remuneration above costs is involved
  - Communications promoting health in general, such as routine tests
  - Communications about government and government-sponsored programs

MentorHealth

New Restrictions on Sale of PHI

- HIPAA §164.508(a)(4): If you disclose for remuneration, you must have an authorization stating that the disclosure results in remuneration
- Exceptions for public health, research, treatment and payment purposes, sale of practice, transfer to a BA providing services, to the individual, etc.
- Worth mentioning in the NPP section on Authorizations

MentorHealth

Fundraising Changes

- Demographic information, dates of healthcare services, department providing services, physician, health plan status, and outcome can be used for fundraising without authorization
- Notice of Privacy Practices must accurately represent what you use: specific PHI or PHI in general
- HIPAA §164.514(f)(1) Opportunity to Opt Out of Fundraising
  - Easy Opt-out must be provided, by campaign or for all campaigns, must be honored, and can't be used to condition treatment or payment

MentorHealth

Individual Access of PHI

- Must have a process for individual to request access, for reasonable cost-based fee
- Must have a process for managing denials of access
- Must provide the entire record in the Designated Record Set if requested:
  - Medical and billing records used in whole or in part to make decisions related to health care
  - Information kept electronically must be available electronically if requested
  - Exceptions for Psychotherapy notes, information for civil, criminal, or administrative proceedings, potential harm, and other specific exceptions
  - Lab results now may be accessed by the individual, effective April 7, 2014
- 30-day extension for offsite data no longer allowed
- Make sure your Notice of Privacy Practices is up to date

MentorHealth

Access and Individual Preferences

- §164.522(b)(1) Standard: Confidential Communications Requirements
  - (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.
- §164.524(c) Provision of Access
  - (2) Form of access requested. (i) The covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual.
  - New (c)(2)(ii): If PHI is electronic, individual may request electronic copy.

MentorHealth

Calculating/Evaluating Risk

- Each Risk Issue has an Impact and Likelihood
  - **Impact** is how great the damage would be; more information about more people with more detail has a greater Impact
  - **Likelihood** is how likely it is that the risk issue would become a reality
- **Risk = Impact x Likelihood**
- If risk level appears low, it may be acceptable to both the entity and the individual
  - An informed risk decision can be made about the importance of mitigating certain risks
  - Rights can not be given up under HIPAA, but individuals can make an informed risk decision

MentorHealth

Changes to Access of Lab Info

- Final Rule with changes to CLIA and HIPAA, enforceable October 4, 2014
- Allows individuals to access results directly from labs
- Impacts:
  - Laboratories will need to establish patient-facing processes
  - Patients may access results without interpretation or counseling
- Final rule available at: https://www.federalregister.gov/articles/2014/02/06/2014-02280/patients-access-to-test-reports-clia-program-and-hipaa-privacy-rule
- Laboratory Notices of Privacy Practices must be updated by now

MentorHealth

Patient Communications

- HHS Guidance and Preamble discussions in new rules say unencrypted e-mail between providers and patients is permitted if the patient requests it, per §164.522, §164.524
- See HHS Guidance, Question 3, page 3: http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf
- See Preamble to Omnibus Update, page 5634: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- See Preamble to CLIA/HIPAA Modifications, page 7302: http://www.gpo.gov/fdsys/pkg/FR-2014-02-06/pdf/2014-02280.pdf

MentorHealth

New Guidance on Access of PHI

- Guidance on Access of PHI, particularly concerning **minors and mental health information:** http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html
- Guidance clarifying that same-sex spouses have the **same HIPAA rights as other family members, no matter where services are provided:** http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/samesexmarriage/index.html

MentorHealth

Impacts of Individual Access of EHR Information

- Updates to your Notice of Privacy Practices
- All kinds of electronic info in designated record set, not just your formal EHR
- Have you performed inventory of PHI?
- Are access Policies and Procedures in place?
- Who responds to requests for access?
- What are acceptable formats for electronic access of PHI?
- Meaningful Use Stage 2 calls for individuals to actually use electronic access of certified EHRs

MentorHealth

Additional Changes to HIPAA: Genetic Information Nondiscrimination Act (GINA)

- New changes to §164.502(a)(5)(i)
- Genetic information not to be used in health plan underwriting, enrollment, eligibility, premium computation, consideration of pre-existing conditions, etc…
- Health Plan Notice of Privacy Practices should have been updated and redistributed by now

MentorHealth

NPP Modifications

- HIPAA Notice of Privacy Practices must reflect individual rights and controls on uses and disclosures
  - New right of access to electronic PHI
  - New right of restriction of disclosures
  - New right to be notified in the event of a breach
  - Changes to Marketing
  - Changes to Fundraising
  - GINA notice for health plan NPPs
  - Changes for Laboratories
  - May remove notice that PHI may be used for Appointment Reminders
- Must update policies and NPP together
- Start using (and post) new version; no requirement for providers to redistribute
- New Samples from HHS (in English and Spanish): http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

MentorHealth

Don't Forget to Customize Your NPP

- Places to put your organization name, affiliates
- Include other uses, such as participating in a Health Information Exchange (which is a treatment thing)
- If your practices are more restricted by state law than by HIPAA, you need to have your NPP reflect that
- The NPP must reflect YOUR privacy practices
- Make sure you have policies and procedures for all that the NPP says you should
- NPP and policies MUST match or one is not valid

MentorHealth

Business Associates Now Directly Regulated by HIPAA

- Security Rule and Breach Notification Rule apply
- Privacy Rule Use and Disclosure provisions apply
- Business Associates responsible for having contracts with Covered Entities and Subcontractors
- Business Associates directly liable for compliance and violations
- Business Associates will need to educate their Subcontractors
- All contracts must meet the new standard now
- New sample Business Associate Agreement template: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

MentorHealth

What is a Business Associate?

- An individual or entity, not acting as an employee, that:
  - Creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA *on behalf of* a covered entity (CE) or another BA
  - Provides legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501), management, administrative, accreditation, or financial services and needs PHI to do it
- Anything a CE could do itself but has someone else do it for them, involving PHI
- Now includes subcontractors, HIEs, Patient Safety Organizations

MentorHealth

What is a Business Associate?

- Includes:
  - Billing, coding services
  - Shredding service
  - Systems vendors who access PHI
  - Technical support services that may access PHI
- Does not include those who would have no reason to be touch PHI:
  - Tradesmen (plumber, etc.)
  - Housekeeping, etc.
  - Conduits (USPS, FedEx, *et al*)
- Not Payers, other Providers, or Workforce Members
- BAs now include subcontractors, Health Information Organizations, and Patient Safety Organizations

MentorHealth

The "Persistence of Custody" Issue and Conduits

- Conduit exception applies only when PHI is not "persistent" in the system
- Conduit exception does not include e-mail services
- Conduit exception does not apply for transfer services that retain copies of PHI
- Encrypted "Cloud" services do not meet the Conduit definition

MentorHealth

EHR System Vendor Questions

- Can disclosures to insurers be properly restricted if requested?
- Can systems provide access to DRS PHI for individuals?
- Does your Business Associate agreement with the vendor supplying your systems require them to provide the abilities you need to meet the new requirements?
- What about proposed changes in Accounting of Disclosures (not in this final rule, but coming someday)?
- Can systems provide an access audit report good enough to satisfy HIPAA Security Rule requirements?

MentorHealth

What is a Breach Under HIPAA?

- Breach is any acquisition, access, use, or disclosure of PHI in violation of Privacy Rule
- Exceptions by law if:
  - PHI is secured (according to HHS guidance) or destroyed
  - Unintentional use, in good faith, with no further use (within your organization)
  - Inadvertent use within job scope (within your organization)
  - Information cannot be retained
- "Harm Standard" for evaluation of need to report removed
- Not reportable if there is a "low probability of compromise" of the data, based on a risk assessment

MentorHealth

Is it a Reportable Breach?

- All breaches not meeting an exception are reportable, unless there is a "low probability of compromise" of the data, based on a risk assessment including at least:
  - what was the info, how well identified was it, and is its release "adverse to the individual"
  - to whom it was disclosed
  - was it actually acquired or viewed
  - the extent of mitigation

MentorHealth

Calculating/Evaluating Risk

- Each Risk Issue has an Impact and Likelihood
  - **Impact** is how great the damage would be; more information about more people with more detail has a greater Impact
  - **Likelihood** is how likely it is that the risk issue would become a reality
- **Risk = Impact x Likelihood**
- Evaluate the Risk of a Compromise (that is, the risk of an access, acquisition, use, or disclosure contrary to rules)

MentorHealth

Is It a Reportable Breach?

Step:	Question:	Answer and Required Action	
1	Was there acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule?	**No**, no acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule; Not Reportable, document the incident and determination; end of process	**Yes**, acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule; Go On to the Next Step
2	Was the information secured according to HHS guidance, or destroyed?	**Yes**, secured or destroyed; Not Reportable, document the incident and determination; end of process	**No**, not secured or destroyed; Go On to the Next Step
3	Was the potential breach a use internal to your organization, that was • unintentional, in good faith, with no further use, or • inadvertent and within job scope?	**Yes**, an internal use exception; Not Reportable, document the incident and determination; end of process	**No**, no internal use exception; Go On to the Next Step
4	Is there no way the breached information can be retained?	**No way** it can be retained; Not Reportable, document the incident and determination; end of process	**Yes**, it could be retained; Go On to the Next Step
5	Does a Risk Assessment show a Low Probability of Compromise? Consider: • what is the data (and how well identified is it) • to whom was it released • was it actually accessed • has it been mitigated	**Yes**, a Low Probability of Compromise; Not Reportable, document the incident and determination; end of process	**No**, NOT a Low Probability of Compromise; Must report the breach; document the incident, determination, & notifications

MentorHealth

Breach Notification Deadlines

- Covered Entities must report breaches to individuals within 60 days
- CEs must report breaches affecting 500 or more individuals to HHS and press within 60 days
- CEs must report breaches of less than 500 to HHS annually by March 1st every year
- If a Business Associate, report to the CE or BA within 60 days
- To file breaches with HHS go to: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
- HHS "Wall of Shame" for large breaches, now easy to search and use: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

MentorHealth

2009-2010 Report on Breaches

- For reported breaches of 500 or more individuals' PHI:
  - 76% of breaches involve loss (15%), theft (56%), or improper disposal (5%) – *Old-fashioned physical security of valuable data!*
  - 17% are caused by unauthorized access or disclosure
  - 6% are caused by hacking
  - Portable data, laptops, smart phones, memory sticks the leaders for large breaches of PHI
- For smaller breaches:
  - Largely single individuals affected (the average small breach affects fewer than 2 individuals)
  - Misdirected fax, e-mail, or hard copy communication: incorrect fax numbers, street addresses, etc.
- See HHS Report to Congress for 2009 and 2010 breaches http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html

MentorHealth

2011-2012 Report on Breaches

- For large breaches, affecting 500 or more individuals:
  - In 2011 and 2012, HHS received 458 reports, affecting 14.69 million people
  - 0.97 percent of reports, but affected 97.89 percent of affected individuals
- For smaller breaches, affecting fewer than 500 individuals:
  - In 2012, there were 21,194 reports, affecting a total of 165,135 individuals
  - In 2012, 83% took place at healthcare providers and 17% at health plans
- How?
  - The most common causes: theft: 53%, and unauthorized access or disclosure: 18%
  - The largest number of individuals affected: due to theft, at 36% of all affected
- Where was the data?
  - Laptop computers (27%), paper (23%), network servers, (13%), desktop computers (12%), and portable electronic devices (9%)

MentorHealth

Lessons Learned From Breaches

- Encrypt whatever you reasonably can; honor wishes of the individuals for communication but explain the risks
- Use physical safeguards
- Increase preparation and vigilance concerning hackers
- Reduce risk through network or enterprise storage as alternative to local devices
- Encrypt data at rest on any desktop or portable device/media storing ePHI – anything that isn't bolted down
- Have clear and well documented administrative and physical safeguards on the portable media which handle ePHI
- Check fax numbers and addresses regularly
- Raise the security awareness of workforce members and managers to promote good data stewardship

MentorHealth

Policy Help

- The SANS Security Policy Project
  - A Short Primer For Developing Security Policies, samples, guidance
  - Available at: http://www.sans.org/resources/policies/
- New York University HIPAA security policies
  - A good level of detail; many of the concepts are directly transferable
  - http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/hipaa-policies.html
- ***NIST Computer Security Incident Handling Guide***
  SP 800-61 Revision 2, a practical guide to responding to incidents and establishing a computer security incident policy and process: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- In addition, the September 2012 ***NIST ITL Bulletin***
  focuses on the revised SP 800-61, available at: http://csrc.nist.gov/publications/nistbul/itlbul2012_09.pdf

MentorHealth

Implementation

- Update Policies and Procedures to match new rights and restrictions
- Update Notice of Privacy Practices to include new changes and required items
  - Be sure to include ALL your privacy practices, even non-HIPAA
  - New Templates from HHS and AMA
    - http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html
    - http://www.ama-assn.org/go/hipaa
- Provide training in new policies and procedures, and the new NPP
- Implement both NPP and P&Ps simultaneously
  - Post new NPP on the wall (or a summary) and Website
  - Have NPP readily available without having to ask
  - Start handing out the new one
  - Providers don't have to mail a new one to everyone

MentorHealth

Training is Essential for Compliance

- Privacy and Security Rules call for training your staff on your policies and procedures and any changes to them
- These are significant changes in the regulations that must be explained to your staff
  - If you are audited the auditors will ask your staff questions
  - Patients may have questions about the new rights
- Use a Multi-Level approach
  - Provide special sessions upon implementation
  - Incorporate into orientation and in-service sessions
  - Include reminders and refreshers
  - Top 10 list of changes for the new HIPAA update
- Document the entire training process – who, what, when

MentorHealth

Documentation: Required & Useful

- Document Policies and Procedures
  - Must realistically represent actual practices
  - Must be within regulatory requirements
- Document any Action, Activity, or Assessment
  - To show policies in place and being used
  - To show good practices
- Make documentation live, accessible, updatable
  - Easy to keep procedures updated
  - Easy to show compliance
  - Use prior questions to evaluate and document your compliance
  - Link all your policies and procedures and documentation to the regulations so they're easy to find for daily use and in the event of an audit or review

MentorHealth

New Enforcement Definitions

- **Reasonable Cause:** An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect
- **Reasonable Diligence:** Business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances
- **Willful Neglect:** Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated

MentorHealth

New Tiered Penalty Structure

- **Tier 1**: Did not know and, with **reasonable diligence**, would not have known
  - $100 - $50,000 per violation
- **Tier 2**: Violation due to **reasonable cause** and not willful neglect
  - $1000 - $50,000 per violation
- **Tier 3**: Violation due to **willful neglect** and corrected within 30 days of when known or should have been known with reasonable diligence
  - $10,000 - $50,000 per violation
- **Tier 4**: Violation due to **willful neglect** and NOT corrected within 30 days of when known or should have been known with reasonable diligence
  - $50,000 per violation
- Can levy fines on a daily basis! $50K per day can add up…
- $1.5 million maximum for all violations of a similar type in a calendar year
- Affirmative Defenses in Tier 1 and Waivers in Tier 2 may be available but **not** when willful neglect is involved

MentorHealth

HHS Is Serious About Enforcement

- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html
- **$4.3 million fine** for Cignet Health of Maryland for **multiple HIPAA violations, including $3 million for willful neglect by ignoring investigators**
- **$1 million settlement** with Mass General Hospital for **records left on the T**
- **$865K+ settlement** with UCLA Medical Center for **snooping in celebrity records**
- **Multi-million dollar settlements** with pharmacies for **poor disposal of PHI**
- **$100K** settlement with a physician's office for **using insecure e-mail & calendar**
- **$1.5 million** settlement with BC/BS of Tennessee for **lost hard drives**
- **$1.7 million** settlement with Alaska Medicaid for **lack of security process**
- **$1.5 million** settlement with MEEI for lack of **security for portable devices**
- **$50K** settlement with Hospice of North Idaho for **insecure laptop, no process**
- **$400K** settlement with Idaho State University for **insecure server, no process**

MentorHealth

HHS Is Serious About Enforcement

- **$275K** settlement with Shasta Regional Medical Center for **inappropriate disclosure of PHI to staff and public, and lack of sanctions for violations**
- **$1.7 million** settlement with WellPoint for **insecure server, no security process**
- **$1.2 million** settlement with Affinity Health for **improper disposal of copiers**
- **$150K** settlement with APDerm for **lost insecure USB drive and no Breach policies**
- **$215K** settlement with Skagit County, WA for **insecure server, no security process**
- **$2 million** in settlements with 2 entities for **unsecured stolen laptops**
- **$4.8 million** in settlements with Columbia/Presbyterian for **poor server management exposing PHI**
- **$800K** settlement with Parkview Health System for **mishandled paper records**
- **$150K** settlement following a breach at Anchorage Community Mental Health Services for **no security processes, not patching system vulnerabilities, and using unsupported software**
- **$125K** settlement with Cornell Prescription Pharmacy for **insecure disposal of PHI**

MentorHealth

Enforcement Lessons Learned

- Information Security Management Process
  - Risk Analysis and Risk Management
  - Incident Handling and Breach Notification
  - Policies and Procedures
  - Training and Documentation
  - Internal Audits and System Reviews
  - Insecure E-mail is a no-no for Professional Communications w/PHI
  - Secure Laptops and Portable Devices
  - Secure System Implementation and Decommissioning Processes

MentorHealth

Enforcement Lessons Learned

- Privacy Rule Compliance
  - Have complete policies and procedures
  - Handle physical records properly, paper and electronic
  - Don’t leave unsecured records in public areas
  - Properly shred discarded paper and pill bottles
  - Have good policies and procedures on how to work outside the office
  - Apply sanctions for violations of HIPAA policies
  - Handle individual requests for records properly
  - Don’t ignore the rules or HHS OCR investigators

MentorHealth

What is a HIPAA Audit?

- HITECH § 13411 requires HHS to conduct periodic audits; initial program in 2012
- New program getting started in 2015
- Will focus on identified problem areas from 2012: laptops, encryption, internal reviews and audits, risk analysis, access of records
- Be able to show you have in place any or all the policies and procedures required by the HIPAA Privacy, Security, and Breach Notification Rules
- Show you have been using them
  - e.g., Show training policy, training materials, and training rosters
  - e.g., Show security incident policy and security incident reports
- ***2 week*** notice! – ***You must be prepared in advance or it's too late!***
- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

MentorHealth

Questions Asked in Prior Audits

- 42 questions asked in first OIG HIPAA Security audit in March 2007 at: http://tinyurl.com/meupq8t
- CMS OESS 2008 Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews, at: http://tinyurl.com/27eakjz
- Questions asked of a small provider after a data breach involving theft of a laptop and server, at: http://tinyurl.com/3jpoa4p
- Questions asked in the first round of 2012 HIPAA random audits (***NOT updated for new rules***), at: http://tinyurl.com/cbcllz7
- HHS OCR 2012 HIPAA Audit Protocol, ***NOT updated for the new rules YET***: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

MentorHealth

2012 HIPAA Audit Program Highlights

- Overall
  - Small covered entities (30% of the sample) had 66% of the deficiencies
  - Health care providers (50% of the sample) had 81% of the deficiencies
  - Security findings were 2/3 of the issues
- Security issues
  - User activity monitoring
  - Contingency planning
  - Authentication/integrity
  - Media reuse and destruction
  - Risk assessment
  - Granting and modifying user access
- Privacy Issues
  - Review process for denials of patient access to records
  - Failure to provide appropriate patient access to records
  - Lack of policies and procedures
  - Uses and disclosures of decedent information
  - Disclosures to personal representatives
  - Business associate contracts

MentorHealth

Method for New Audits

- To be done by HHS Office for Civil Rights staff
- Find audit targets through survey of 1200 entities
- Approximately 200 Desk audits of specific issues, not general
- Will be more specific to particular **problem areas revealed in Breaches, Enforcement Actions, and the 2012 Audits – *Learn your lessons!***
  - All communication, submissions electronic, via portal
  - **NO CHANCE to provide additional information – you must provide what is needed the first time**
- Field audits as necessary, approximately 200, more comprehensive
- Get list of Business Associates from initial audit targets
- Audit Covered Entities, and then their Business Associates

MentorHealth

And it's not just HHS OCR…

- HHS Office of Inspector General will also be auditing HIPAA Security Rule compliance including:
  - Analyzing the IT security of community health centers funded by the Health Resources and Services Administration
  - Reviewing controls over networked medical devices at hospitals.
  - The HHS OIG Work Plan for Fiscal Year 2015 is available at: http://oig.hhs.gov/reports-and-publications/archives/workplan/2015/FY15-Work-Plan.pdf
- And don't forget the Meaningful Use audits for EHR Incentive Funding, verifying you have performed a HIPAA Security Rule Risk Analysis

MentorHealth

Your to-do list…

- Don't be in denial – willful neglect will costs more than compliance
- Review your policies and procedures per the new rights and restrictions
- Update your policies and Notice of Privacy Practices
- Review Business Associate Agreements
- Make sure EHR vendors can meet restriction requirements and provide electronic copies
- Prepare for Breach Notification
- Review the questions asked in prior HIPAA audits
- Be ready for incidents and audits – conduct drills
- Provide training and document compliance
- Always have a plan for moving forward, and follow it!

MentorHealth

Thank You!

- **News items**, as well as numerous **resources, regulations, laws, guidance, and tools,** of interest to those involved with health information privacy and security regulatory compliance are available without charge or registration at:

  www.lewiscreeksystems.com

MentorHealth

Questions

- If there are any further questions which we were not able to get to today please feel free to contact me through MentorHealth

Or, contact me at:

Jim Sheldon-Dean
Lewis Creek Systems, LLC
5675 Spear Street, Charlotte, VT 05445
jim@lewiscreeksystems.com
www.lewiscreeksystems.com

MentorHealth

Upcoming Events from Jim Sheldon-Dean

New HIPAA Compliance Audit Program –
The New Audit Protocol and How It Affects You

Thursday, July 16, 2015, 10:00 AM PDT | 01:00 PM EDT, Duration: 90 Minutes

http://www.mentorhealth.com/control/w_product/~product_id=800460LIVE

MentorHealth

Contact Us:

- *Customer Support at : 1.800.447.9407*
- *Questions/comments/suggestions: webinars@mentorhealth.com*
- *Partners & Resellers: partner@mentorhealth.com*