MentorHealth

Live Webinar
on

Texting and E-mail: Communication Options with Patients to Meet Their Needs and Desires under HIPAA Rules

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

November 10, 2015

www.mentorhealth.com
1

MentorHealth

Agenda

- Discuss how to handle patient communications
- Discuss how E-mail and Texting can work under HIPAA
- Identify guidance from HHS for patient communications
- Identify HIPAA policies that need to be changed
- Discuss new rights for electronic copies of electronic records
- Show the new process that must be used in the event of breach
- Learn about being prepared for enforcement and auditing
- Learn how to approach compliance
- Q&A session

www.mentorhealth.com
2

Jim Sheldon-Dean
Lewis Creek Systems, LLC
802-425-3839 jim@lewiscreeksystems.com

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.

www.mentorhealth.com 3

MentorHealth

HIPAA Privacy and Security Rules

- HIPAA Privacy Rule
  - 45 CFR § 164.5xx
  - Enforceable since 2003
  - Establishes Rights of Individuals
  - Controls on Uses and Disclosures
- HIPAA 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
- Enforcement a recent priority
- Rules now applicable to HIPAA Business Associates

www.mentorhealth.com 4

MentorHealth

HIPAA Breach Notification Rule

- Breach Notification Rule
  - 45 CFR § 164.4xx
  - Enforceable since February 2010, Final Rule now in effect, with changes in how to determine if a breach must be reported (2013)
  - Requires reporting of all PHI breaches to HHS and individuals
  - Extensive/expensive obligations
  - Provides examples of what ***not*** to do on the HHS "Wall of Shame": https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- 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

www.mentorhealth.com 5

MentorHealth

So, what are we allowed to do?

- Do what the patient wants
  - Meet HIPAA Requirements
  - Accommodate what you reasonably can
- Do what you can handle properly
  - For Patient Care
  - For Medical Records

www.mentorhealth.com 6

MentorHealth

Why might patients wish to communicate?

- Communication with the office
  - Prescription Renewals
  - Scheduling
  - Questions
  - Continuing conversations with the doctor
- Discussion of particular health issues
- Access of Medical Records, test results

www.mentorhealth.com 7

MentorHealth

What are the HIPAA considerations?

- HIPAA Security Rule §164.312(e) requires consideration of encryption of communications as an Addressable Implementation Specification
- HIPAA Privacy Rule §164.522 and §164.524 give patients rights of communication preferences and access of information
- Making Patients happy
- Making HHS happy

www.mentorhealth.com 8

Jim Sheldon-Dean
Lewis Creek Systems, LLC
802-425-3839 jim@lewiscreeksystems.com

MentorHealth

Professional Communications MUST be protected

- Required HIPAA Risk Analysis shows risks of using insecure communications such as plain e-mail and texting
- Organizations that discover they have used insecure communications report insecure communications as a breach
- One of the enforcement settlements was based in part on the use of insecure e-mail for professional communications http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf

www.mentorhealth.com 9

MentorHealth

Communication with Patients requires flexibility

- Provide a variety of means of communication that you understand and manage
- Provide and encourage using secure solutions for communications
- Be prepared to respond to requests to do other than your preferences
- Need to have policies and processes for such decisions, and documentation

www.mentorhealth.com 10

MentorHealth

E-mail, Texting, and Security

- E-mail and texting are inherently insecure
- Unless steps are taken, e-mail and texts may be retained or exposed by unknown parties
- Secure communications are essentially required as good practice for professional communications
- Yahoo mail, g-mail, texting, etc., are all insecure means of communication and their use may be considered a breach
- Technologies for securing communications are readily available today

www.mentorhealth.com 11

MentorHealth

Many Prefer E-mail to Telephone

- Scheduling
- Reporting of status
- Inquiries about issues, treatments
- Requesting copies of records
- Communication of test results
- Can be more accurate than the phone
- Provides a documented record of communication

www.mentorhealth.com 12

MentorHealth

What can go wrong with E-mail

- Communications are not secured by default and may be retained or exposed by unknown parties
- Secure e-mail solutions for general use are often cumbersome
- No real assurances of privacy and security in the chain of communications
- An individual's e-mail could be accessed by a third party if a weak or easy-to-guess password is used for the e-mail account

www.mentorhealth.com 13

MentorHealth

Texting is Very Useful

- Fast way to communicate short messages
  - Useful for Updates, Schedule Changes
  - Easy to communicate if running late, etc.
  - Quick communication of results, comments
- More appropriate than an e-mail or phone call
  - Can be more discreet and private than a phone conversation
  - Can be quicker than a phone call for short messages
  - Can provide accurate information not dependent on voice
- Many communications used to go by Pager
  - Many paging operations moving to texting now
  - Texting is more interactive than paging

www.mentorhealth.com 14

MentorHealth

Potential Mobile Device Issues

- Information provided to the wrong individual through poor authentication and access control, leading to a "small" breach and a healthcare threat
- Incorrect information provided about an individual, perhaps by faulty authentication or a poorly performing App, causing a healthcare threat
- Patient loses control of device exposing their data (their problem) and potentially exposing additional data or providing faulty data (whose problem?)
- Provider loses control of device potentially exposing extensive data (big problem) and potentially providing access to provider systems (bigger problem)
- Data travels through insecure channels and may remain, accessible, on systems

www.mentorhealth.com 15

MentorHealth

Three Issues with Texting

- It's a Privacy thing: Patients may not appreciate the risks of loss of privacy
  - HIPAA requires you to do your best to meet patient preferences for communication method
  - Use Risk Analysis to evaluate and explain risks
  - It's a new technology and people will not understand it fully for quite some time
- It's a Medical Records thing: Documentation is key to health care
  - Regular texting doesn't provide a paper trail of conversations and contacts
  - If it's part of patient care, it must be documented properly
  - Secure, traceable texting is essential when medical record information is texted
- It's a patient safety thing: Triage of incoming messages is essential
  - Regular texting doesn't automatically route to the most appropriate individual
  - Texts may arrive at all hours, 24/7 and may include a variety of information and situations, including emergencies
  - Texting with patients must be managed to protect patients and provide appropriate service

www.mentorhealth.com 16

Jim Sheldon-Dean
Lewis Creek Systems, LLC
802-425-3839 jim@lewiscreeksystems.com

MentorHealth

Secure Texting Solutions

- Cortext by Imprivata
  - Comes in several versions; Free app provides a secure channel
  - Upgrades provide documentation, reporting, etc.
  - http://www.imprivata.com/secure-messaging
- TigerText
  - Free app provides a secure channel
  - http://www.tigertext.com/messaging-for-healthcare/
- DocHalo – http://www.dochalo.com/secure-texting.html
- OhMD – http://www.ohmd.com
  - App for Individuals (Patients) is free
  - Office implementation integrates with the EHR
  - Messages go to team for Triage
  - Fantastic acceptance:
    - 90% of individuals prefer it to a phone call
    - 86% of individuals that download it use it
    - 80% of providers say it's easier than a phone call

www.mentorhealth.com 17

MentorHealth

Designated Record Set

In 45 CFR §164.501:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

www.mentorhealth.com 18

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, 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
- Access of PHI by individuals is a HOT BUTTON issue for HHS

www.mentorhealth.com 19

MentorHealth

Steer Patients to your Portal

- Most new EHR systems offer a Portal option for patients to use to access their records in the EHR; encourage them to use the Portal
- The EHR may not reflect all of the information in the Designated Record Set
- Be prepared to handle requests for information in the DRS outside the EHR
- You must accommodate reasonable requests to communicate by other means
- Be careful in setting costs for electronic copies of records!

www.mentorhealth.com 20

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.

www.mentorhealth.com 21

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

www.mentorhealth.com 22

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

www.mentorhealth.com 23

MentorHealth

Impacts of Individual Access of EHR Information

- Updated the 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

www.mentorhealth.com 24

MentorHealth

Policy on Using Insecure Communications with Patients

- Insecure communications are prohibited for professionals
- Define the usual, preferred, secure means of communication, and the preferred insecure alternatives
  - Consider what you are "reasonably able" to do
- Require patient to request using insecure communication methods, and indicate preferred method to be used
- If another method is requested, consider it according to § 164.522(b)(2) and § 164.524(c) and guidance
- If an insecure alternative method is granted:
  - Explain risks
  - Obtain consent (with signature if appropriate)
  - Inform those who communicate of the preference
- Document the request and consent or denial

www.mentorhealth.com 25

MentorHealth

Information Security Management Process

- Definition of Information Security – Protecting:
  - ✓ Confidentiality
  - ✓ Integrity
  - ✓ Availability
- Definition of a Management Process:
  - ✓ Define and understand what you have
  - ✓ See how well it performs
  - ✓ Watch for problems
  - ✓ Review activities and issues
  - ✓ Make changes based on bang-for-buck

www.mentorhealth.com 26

MentorHealth

Information Security Management Process

- ✓ Information Inventory and Flow Analysis
- ✓ Access and Configuration Control
- ✓ Know who and what's been going on in your networks and systems
- ✓ Respond to and learn from Incidents
- ✓ Audit and review regularly, and when operations or environment change
- ✓ Make risk-based improvements
- ✓ Focus: Confidentiality, Integrity, Availability

www.mentorhealth.com 27

MentorHealth

Risk Analysis Guidance

- July 14, 2010 final guidance issued
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- Basics of Risk Analysis and Risk Management from HHS
  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf
  - Identifies National Institute of Standards and Technology (NIST) Special Publication SP 800-30 for methodology (use this older version, NOT the newer Rev. 1 version)
    http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
  - Identifies NIST SP 800-66 as a guide to HIPAA compliance and relevant NIST documents to support compliance
    http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- NIST HIPAA Security Rule Toolkit: http://scap.nist.gov/hipaa/
- ONCHIT/OCR/OGC Security Risk Assessment Tool for iPad and Windows 7
  http://www.healthit.gov/providers-professionals/security-risk-assessment

www.mentorhealth.com 28

MentorHealth

Portable Technology Policy

- Responsibility to use devices securely
  - Physical and technical security
- Must protect devices and any PHI on them
  - Good passcodes and encryption
- IT approval for access; required settings
  - Auto-wiping and remote wiping
- Security of passwords
- Don't intermingle personal and patient e-mail & texts
- Remote Use of PHI is subject to controls
- Must inform manager if lost or stolen
- Must have device cleared of any PHI prior to trade-in

www.mentorhealth.com 29

MentorHealth

Security Policy Framework

- Cover the Administrative, Physical, and Technical Safeguards
- Four Basic Policies or Policy Types
  - Security Management Process
  - Information Access Controls
  - Data Management (Contingency-Backup-Retention)
  - User Policy
- Include enabling language in Policy
- Define details in Procedures
- Documentation, Documentation, Documentation

www.mentorhealth.com 30

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

www.mentorhealth.com 31

MentorHealth

What is a Breach Under HIPAA?

- §164.402 Breach is any acquisition, access, use, or disclosure in violation of the Privacy Rule, except if:
  - Unintentional internal use, in good faith, with no further use
  - Inadvertent internal use, within job scope
  - Information cannot be retained (returned intact, unopened, unviewed)
- Not Reportable if:
  - Secured (encrypted) or destroyed
- Otherwise: Reportable unless there is a "low probability of compromise" based on a risk assessment, examining at least:
  1. what was the info, how well identified was it, and is its release "adverse to the individual"
  2. to whom it was disclosed
  3. was it actually acquired or viewed
  4. the extent of mitigation

www.mentorhealth.com 32

MentorHealth

Calculating/Evaluating Risk of Compromise

- **Compromise:** An acquisition, access, use, or disclosure in violation of the Privacy Rule not meeting an exception
- 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**

www.mentorhealth.com 33

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

www.mentorhealth.com 34

MentorHealth

Breach Notification Deadlines

- All breaches, large and small, are reportable to the individuals promptly, within 60 days
- Breaches affecting 500 or more individuals must also be reported to HHS and the press within 60 days of discovery
- Within 60 days of the end of every year: Report all prior year's small breaches to HHS
- Be sure to include commentary on what you have done to mitigate the issue, prevent it from happening again, and verify your success
- Business Associates must report incidents and breaches to the entities that hire them within 60 days
- To file breaches with HHS go to: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

www.mentorhealth.com 35

MentorHealth

Reports to Congress on Breaches

- 2009-2010 Report
  - 76% of large breaches (>500 affected) involve loss (15%), theft (56%), or improper disposal (5%) – *Old-fashioned physical security of valuable data!*
  - Portable data, laptops, smart phones, memory sticks the leaders for large breaches of PHI
  - For smaller breaches, largely single individuals affected: misdirected fax, e-mail, or hard copy communication
- 2011-2012 Report
  - Large breaches (>500 affected) are 0.97 percent of reports, but affected 97.89 percent of affected individuals
  - Laptops and portable electronic devices represent 36% of breaches
  - 83% of smaller breaches take place at healthcare providers
- See HHS Reports to Congress on HIPAA breaches http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html

www.mentorhealth.com 36

MentorHealth

Lessons Learned From Breaches

- **Encrypt data** at rest on any desktop or portable device/media storing EPHI
- Have clear and well documented **administrative and physical safeguards** on the storage devices and removable media which handle EPHI
- Raise the **security awareness** of workforce members and managers to promote good data stewardship
- Make sure you have the **right fax number** or e-mail or postal address
- Do not neglect **physical safeguards** for areas where paper records are stored or used
- Reduce risk through **network or enterprise storage** as alternative to local devices
- **Monitor and audit** your systems so you know what's going on

www.mentorhealth.com 37

MentorHealth

What is a HIPAA Audit?

- HITECH § 13411 now requires HHS to conduct periodic audits
- Initial program conducted in 2012, being revised
- Will focus on identified problem areas from 2012 and in breach reports
- **Show you have considered Texting and E-mail in your Risk Analysis and have applied appropriate physical, technical & administrative safeguards**
- Show you have in place all the policies and procedures required by the HIPAA Privacy and Security 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
- ***Now just 2 week notice – You must be prepared in advance or it's too late!***
- See: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html

www.mentorhealth.com 38

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

www.mentorhealth.com 39

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

www.mentorhealth.com 40

MentorHealth

Method for New Audits

- Contact information for potential Audit targets being verified now
- Approximately 200-350 Desk audits of specific issues, not everything
  - By HHS Auditors, with assistance from an outside vendor
  - All communication, submissions electronic
  - **NO CHANCE to provide additional information – you must provide what is needed the first time**
- Field audits as necessary, approximately 200, depending on budget
- Get list of Business Associates from audit targets
- Audit Covered Entities, and then their Business Associates
- **E-mail and Texting: new target area, in addition to Access?**

www.mentorhealth.com 41

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 security at recipients of Meaningful Use funding
  - 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

www.mentorhealth.com 42

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

www.mentorhealth.com 43

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

www.mentorhealth.com 44

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**
- **$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**
- **And that's not all…**

www.mentorhealth.com 45

MentorHealth

HHS Is Serious About Enforcement

- **$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 after a breach at Anchorage Community Mental Health Services for **no security processes, not patching systems, and using unsupported software**
- **$125K** settlement with Cornell Prescription Pharmacy for **insecure disposal of PHI**
- **$218K** settlement with St. Elizabeth's Medical Center for using **web-based storage without risk analysis**, and **breach of information on a laptop** held by a former employee
- **$750K** settlement with Cancer Care Group, P.C. for **unencrypted, stolen laptop & backup, no Risk Analysis or Risk Management Plan, no Policies on portable devices**
- **And more to come!**

www.mentorhealth.com 46

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
  - Secure Laptops and Portable Devices
  - Secure System Implementation and Decommissioning Processes

www.mentorhealth.com 47

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

www.mentorhealth.com 48

Jim Sheldon-Dean
Lewis Creek Systems, LLC
802-425-3839 jim@lewiscreeksystems.com

MentorHealth

First: Secure Data at Rest & in Motion

- Laptops, smart phones, CDs, memory sticks,… use Mobile Device Management policies and tools to control access and storage of PHI
- Desktops and servers can be stolen; encrypt what can be carried out of your office with PHI
- Copiers and printers with hard drives must not be returned to the leasing company with PHI
- Do NOT use unencrypted e-mail for professional communications

www.mentorhealth.com 49

MentorHealth

Second: Train Your Staff

- Make sure they know what to do
  - For information security, especially portable devices and working outside of the office
  - For proper handling of PHI in paper and electronic formats
  - For proper disposal of physical and electronic PHI
  - For exercise of patient rights such as access
  - For interaction with family, friends, personal representatives
  - For issues with minors
  - For handling PHI of the deceased

www.mentorhealth.com 50

MentorHealth

Third: Establish Your Information Security Management Process

- Risk Analysis and Risk Management
- Incident Handling and Breach Notification
- Policies & Procedures, Training & Documentation
- Internal Audits and System Reviews
- User access controls and activity monitoring
- Contingency planning
- Authentication/integrity
- Media reuse and destruction
- Business Associate Agreements

www.mentorhealth.com 51

MentorHealth

Fourth: Follow Through

- Make sure your policies and procedures match the updated HIPAA Privacy and Breach Rules under HITECH
- Keep your training up to date
- Be prepared to apply sanctions if necessary
- Schedule your Information Security Management Process activities, such as:
  - Reviews of security and compliance
  - Reviews of access by staff
  - Incident Reviews
  - Verification of fax numbers and addresses
  - Update of the Risk Analysis

www.mentorhealth.com 52

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 a tool such as the NIST HIPAA Security Rule Toolkit, or the HHS Office for Civil Rights HIPAA Audit Protocol
  - 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

www.mentorhealth.com 53

MentorHealth

Audit Your Own Compliance

- Ensure your Policies and Notice of Privacy Practices reflect the recent changes in the rules ***and your own practices***
- Make sure you handle any denials of access properly
  - Process for reviews of reviewable denials
- Make sure your fees do not exceed either HIPAA or state maximum
- Review your practices regularly to determine if your preferred practices are working
  - Make sure there is consent for the use of insecure communications
  - Verify documentation of insecure uses
- Review any exceptions to the preferred practices
- Verify that secure communications are used for all professional-to-professional communications

www.mentorhealth.com 54

MentorHealth

Where do we start?

- Find out what people are doing already
- Consider professional communications and patient communications separately
- Document your processes for proper methods of communications with both patients and professionals
- Find ways to secure professional communications
- Find ways to offer secure patient communications
- Develop and document the process for adopting and using insecure communications (plain e-mail or texting) if patients desire
- Have a clear process for discussion of risks and indication of patient desires, with documentation

www.mentorhealth.com 55

MentorHealth

Your to-do list…

- Don't be in denial – willful neglect costs more than compliance
- Accommodate new individual rights
- Review and update your policies and procedures per the rules
- Establish your processes for Risk Analysis and Documentation
- Document your communications policies and procedures
- Update your Notice of Privacy Practices
- Train staff in new policies and procedures
- Document, document, document!
- Conduct drills in audit and breach response
- Make corrections based on results
- Always have a plan for moving forward, and follow it!

www.mentorhealth.com 56

MentorHealth

Thank You!

- **News items** of interest to those involved with health information privacy and security regulatory compliance, as well as numerous **resources, regulations, laws, guidance, and tools** 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

Global Compliance Panel 2-day In-person Seminar –

Texting and E-mail with Patients: Patient Requests and Complying with HIPAA

Thursday December 3 – Friday December 4, 2015 in Baltimore, Maryland

https://www.globalcompliancepanel.com/control/globalseminars/~product_id=900313SEMINAR?HIPAA-texting-email-patients

New HIPAA Audit and Enforcement Activities: Being Prepared to Show your Compliance

Webinar, Tuesday, December 15, 2015, 10:00 AM PST | 01:00 PM EST, Duration: 90 Minutes

http://www.mentorhealth.com/control/w_product/~product_id=800578LIVE

www.mentorhealth.com 59

MentorHealth

Contact Us:

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

www.mentorhealth.com 60