

**Patient Rights Drive Practice Responsibilities:  
Understanding New Information Release  
Requirements**

*Rita K. Bowen, MA, RHIA, CHPS, SSGB  
Sr. VP HIM and Privacy Officer, HealthPort*

*Alisha R. Smith, RHIA  
HIM/Compliance Educator, HealthPort*

---

---

---

---

---

---

---

---

**Agenda**

**What's the Same and What's New**

- New Patient Rights
- Quantifying noncompliance risk
- Measuring impact on your practice

**Practical steps for Information Release Compliance**

- Revising intake and patient management workflows
- Creating new operational checklists
- Assessing and modifying practice management/EMR/E-HR systems
- Complying with Omnibus while also supporting complete documentation and continuity of care

**Meaningful Use Stage 2**

**Meaningful Use & Patient Portals**

**View, Download, Transfer**

**HIE & How to Properly Prepare**

**Conclusion/Questions**

---

---

---

---

---

---

---

---

**What's the Same and What's New**

**New Patient Rights**

---

---

---

---

---

---

---

---

**Electronic Copy of PHI**

- Form and Format requested, if readily producible – electronically (patients can receive their information in a more convenient and accessible format)
- If not readily producible and maintained in paper, then readable hard copy

---

---

---

---

---

---

---

---

**Patient may make request for their health information in a specific form or format, but only if:**

- Provider or plan is capable of producing in requested format, for example:
  - MS Word
  - Excel
  - Text
  - HTML
  - PDF

---

---

---

---

---

---

---

---

**Copy of PHI to Third Parties**

- Individual may designate third party to receive copy
  - Must be in writing
  - Clearly identify the designated person
  - Clearly identify where to send the copy
- Request VS Authorization: Who is making the request?

---

---

---

---

---

---

---

---

**If the patient opts out of secure transmission/e-mail**

- The covered entity or plan must notify the patient that there is "some level of risk that the information in the e-mail could be read by a third party"
  - Best practice suggests that you maintain notification with the patient's indication to opt out
  - New form may need to be introduced and location for documentation to be maintained

---

---

---

---

---

---

---

---

**Fees for all**

- Costs, or
- State law's per page rate
  - *WHICH EVER IS LESS*

---

---

---

---

---

---

---

---

**Response Time Expectations**

- The final rule shortens the turnaround time for producing records (i) to a patient or (ii) by patient request to be sent to someone else to 60 days. Previously the law allowed a total of 90 days to produce records when a patient requested them – 30 days if the records were on-site at the facility, plus 60 days if the record was stored off-site. The new law still allows (no change) 30 days if the records are on-site, *but shortens the time for producing records that are off-site to 30 additional days, for a total of 60 days.*

---

---

---

---

---

---

---

---

**Restriction for Out-of Pocket Payments**

- Covered entity must agree to individual's request to restrict disclosure to health plan
  - For payment or health care operations
  - Unless disclosure is required by law
  - If individual (or third party) pays for item or service out of pocket in full

---

---

---

---

---

---

---

---

**Health Information of Deceased Individuals**

- **Standard 164.502 (f)**
  - A covered entity **must** comply with the requirements of the HIPAA privacy rule with respect to the protected health information of a deceased individual *for a period of 50 years following the death of the individual*

---

---

---

---

---

---

---

---

**Decedent Information to family member or other involved in care**

- Covered entity may disclose PHI to persons involved in decedent's care or payment unless prior expressed preference of the individual is known to the covered entity **164.501 (b) (5) and** provided the information released is relevant to such person's involvement

---

---

---

---

---

---

---

---

**No longer PHI 50 years after death - Exceptions**

- The Rule does not override or interfere with State or other laws that provide greater protection of such information or the professional responsibilities of mental health or other providers.
- This is not a record retention requirement..covered entities may choose to destroy decedent information although other applicable law may prescribe or limit such destruction.

---

---

---

---

---

---

---

---

**Childhood Immunizations**

- Covered entity may release student immunization records to school without authorization
  - If state law requires school to have immunization record (state where school is located)
  - Written or oral agreement (must be documented)

---

---

---

---

---

---

---

---

**Disclosure and Sale of PHI**

- New restriction on disclosures that describe item or service when covered entity receives financial remuneration from third party whose item or service is described.

---

---

---

---

---

---

---

---

**Documentation:  
Risk Determination Phase or Likelihood of Occurrence Levels**

Likelihood	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years.
Low	Likely to occur one every year or less.
Medium	Likely to occur once every six months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month
Extreme	Likely to occur multiple times per day

---

---

---

---

---

---

---

---

---

---

---

---

**Documentation of Risk Determination Phase:  
Impact Severity Levels**

Impact Severity	Description
Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of Government information or services.
Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.

---

---

---

---

---

---

---

---

---

---

---

---

"Ladies and Gentlemen, I wish I had better news for you but we are facing a storm that most of us have feared. This is a threat that we've never faced before." (Ray Wagin)




---

---

---

---

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers**

- **Continuing Failure to Encrypt Data and Devices**
  - Data Should be encrypted at rest and in transit
  - If decision is made that certain data or data storage devices cannot be encrypted, documentation of reasons and selection of alternative are critical
  - Use strong passwords
- **BYOD: Bring Your Own Device**
  - Policies need to address
    - Type of data that can be used on mobile devices
    - Identify of authorized users, and limitations with respect to the mobile devices, and
    - Security of those devices

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers**

- **BYOD: Bring Your Own Device**
  - Users need to understand that using personal mobile devices for business purposes imposes additional obligations on the user and may require the implementation of technology on the device
- **Cloud storage**
  - Begins with selection of cloud provider and continues through the contract negotiation process
  - Critical that the level of security provided by a cloud provider is properly matched to the level of security needed by the type of data to be stored and/or processed in the cloud
  - Any cloud vender that receives, creates, maintains, stores, or processes PHI, even if encrypted, needs to sign a business associate agreement

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers**

- **Business Associates**
  - Ensure that business associates understand their obligations with respect to the protection of data and the reporting of breaches
  - Ensure that a business associate agreement is in place for all business associates and that it has been properly updated as required
  - Ensure that an P&S Incident response plan is in place by the BA
- **Networked Medical Devices**
  - Include medical devices in risk assessment
  - Work with medical device companies to determine how best to implement critical security updates and patches
  - Monitor medical devices for indication of compromise, medical device passwords should be checked and, if possible, default passwords changed to unique passwords.

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers**

- **Malware**
  - Unless you are expecting to receive an email (phishing occurs in text messaging as well) containing a link or asking for sensitive information, don't respond
  - Check actual address of link or website, and be careful what information is shared
  - If the facility has a Bring Your Own Device (BYOD) policy, consider only permitting vetted applications on mobile devices that attach to organization's network

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers**

- **Social Media**
  - Ensure that organization has a reasonable and well-known social media policy
  - Policy needs to define the parameters of social media use on behalf of organization and who is permitted to represent organization in social media
  - Individual should be identified who can answer questions regarding who can use which forms of social media
  - Ensure that your social sites use strong passwords
- **People**
  - Critical to adopt good privacy and security practices from the top down and to ensure that each employee understands that their actions and good computer security is a personal responsibility, which has a direct impact on the organization

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers: Privacy & Security Breaches**

- January 2013 Health Information Technology Omnibus rules
  - provision with the most immediate and widespread impact has been new breach notification rule, due to continuing volume of security breaches
- Challenge for health-care industry is to improve privacy and security practices and try to reduce extent of breaches
  - every business faces realistic risks of privacy and security breaches;
  - these breaches result in complicated analysis and regulatory and operational challenges, resulting from contractual entanglements and numerous state laws; and
  - many of these breaches could have been prevented through more effective security practices

---

---

---

---

---

---

---

---



**Quantifying noncompliance risk for Health Care Providers: Privacy & Security Breaches by Insiders**

- Breaches resulting from improper behavior by employees who need access to data to do their jobs but then misuse this data for an inappropriate purpose
  - Review of medical records of celebrities or other individuals with personal connections to an employee
  - More malicious situations where employees misuse data to commit identity theft, engage in fraud or otherwise misuse or wrongfully disclose sensitive personal information
- Need to take steps up front to reduce risks, and then engage in Ongoing activities to monitor and investigate

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers: Privacy & Security re: Mobile Devices**

- Organizations that have not yet developed an appropriate policy for the use of mobile devices have in fact adopted a policy
  - letting data be used and disclosed in largely unpoliced ways
- Broad range of concerns:
  - theft of personal and corporate data
  - overall employee monitoring strategies
  - new and expanding risks from security breaches and need to be investigated

---

---

---

---

---

---

---

---

**Quantifying noncompliance risk for Health Care Providers: Privacy & Security - Photocopiers**

- Began when Affinity was advised by CBS Evening News that CBS had purchased a photocopier previously leased by Affinity
  - Copier's hard drive contained confidential medical information relating to Affinity patients
  - As a result, on August 15, 2010, Affinity self-reported a breach with the HHS' Office for Civil Rights (OCR)
  - Affinity estimated that the medical records of approximately 344,000 persons may have been affected by this breach
- **\$1,215,780** settlement with Affinity Health Plan, Inc., arising from an investigation of potential HIPAA violations

---

---

---

---

---

---

---

---

**Privacy and Security – Photocopiers, continued**

- Determined that Affinity had failed to incorporate photocopier hard drives into definition of electronic protected health information in risk assessments required by the Security Rule
- Failed to implement appropriate policies and procedures to scrub internal hard drives when returning photocopies to its office equipment vendors
- Determined that Affinity also violated the Privacy Rule
- Requires implementation of a Corrective Action Plan
  - Must use best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent... and take protective measures to safeguards all ePHI going forward ..

---

---

---

---

---

---

---

---

**Audit Expectations**

**"It is better to meet danger than wait for it. He that is on the shore, and foresees a hurricane, stands out to sea and encounters a storm to avoid a ship wreck."**  
 (Charles Caleb Colton)




---

---

---

---

---

---

---

---

**Privacy and Security Audit Expectation – measuring impact on your practice**

- Audits are conducted using audit trails and audit logs that offer a back-end view of system use. Audit trails and logs record key activities, showing system threads of access, changes, and transactions. Periodic reviews of audit logs may be useful for:
  - Detecting unauthorized access to patient information
  - Establishing a culture of responsibility and accountability
  - Reducing the risk associated with inappropriate accesses (behavior may be altered when individuals know they are being monitored)
  - Providing forensic evidence during investigations of suspected and known security incidents and breaches to patient privacy, especially if sanctions against a workforce member, business associate, or other contracted agent will be applied
  - Tracking disclosures of PHI

---

---

---

---

---

---

---

---

**Privacy and Security Audit Expectation – measuring impact on your practice**

- Responding to patient privacy concerns regarding unauthorized access by family members, friends, or others
- Evaluating the overall effectiveness of policy and user education regarding appropriate access and use of patient information (comparing actual worker activity to expected activity and discovering where additional training or education may be necessary to reduce errors)
- Detecting new threats and intrusion attempts
- Identifying potential problems
- Addressing compliance with regulatory and accreditation requirements

---

---

---

---

---

---

---

---

**Audits... prepare & review Measuring impact on your practice**

"You got to be willing to walk in a storm.  
That's what I tell people all the time." (Ray Lewis)



---

---

---

---

---

---

---

---

**Determining What to Audit - Measuring impact on your practice**

- It would be prohibitive to perform security audits on all data collected. Good-faith efforts to investigate the compliance level of individuals educated on privacy and information security issues can be achieved through a well-planned approach.
- In determining what to audit, organizations must identify and define "trigger events," or the criteria that will flag questionable access of confidential ePHI and prompt further investigation. Some triggers will be appropriate to the whole organization, while others will be specific to a department or unit. Once identified, trigger events should be reviewed on a regular basis, such as annually, and updated as needed.<sup>1</sup>

---

---

---

---

---

---

---

---

**Measuring impact on your practice**

- 1) Enhance administrative controls
- 2) Monitor physical and system access
- 3) Identify workstation usage
- 4) Audit and monitor system users
- 5) Employ device media controls
- 6) Apply data encryption

---

---

---

---

---

---

---

---

**Measuring impact on your practice - BAs**

- Rules implemented direction of the HITECH law from 2009, the reality is that , in 2014, for first time, all HIPAA business associates will face full obligation to follow the HIPAA rules

Requires:

- Proactively investigation of potentially suspicious behavior, &**
- Improve inventory accountability**

---

---

---

---

---

---

---

---

**Measuring impact on your practice - BAs**

- HIPAA business associates, and all downstream subcontractors, must have
  - Effective compliance plans to meet all contractual obligations of a HIPAA business associate agreement
  - Full and complete set of compliance policies and procedures related to the detailed obligations of the HIPAA privacy and security rule. It is clear that business associates, like covered entities, are not one size fits all
  - Some entities, such as document storage companies and cloud providers, may have no reason to know whether they maintain PHI at all, or at least have any idea what PHI they do maintain

---

---

---

---

---

---

---

---

**Measuring impact on your practice - BAs**

3 steps critical to maintaining or developing appropriate compliance programs:

1. Developing an appropriate privacy and security program that both effectively protects PHI and that is reflected in reasonable documentation;
2. Program to act quickly in event of a privacy or security breach, to investigate the breach, mitigate potential harm and provide appropriate notification; and
3. Assessment of where the HIPAA rule (privacy and security) requirements matter most, which will vary significantly based on the particular services being provided

---

---

---

---

---

---

---

---

"Remember, the storm is a good opportunity for the pine and cypress to show their strength and their stability" (Ho Chi Minh)

Thus why we should audit to OCR's Focus areas



---

---

---

---

---

---

---

---

**FOCUS for OCR Audits - Measuring impact on your practice - BAs**

- A consistent message regarding privacy and security
- A consistent corrective disciplinary action (thus the accountability matrix)
- Compliance and Integrity of the program
  - Enhanced Public Trust
  - Strengthened response to legal actions
  - Strengthened response to penalties and/or fines

---

---

---

---

---

---

---

---

**FOCUS for OCR Audits - Measuring impact on your practice**

- Conduct internal assessments of privacy and security programs
- Review Breach Detection and Notification processes
- Assure Policy and Procedures up to date
- Observe staff adherence to the written P&P
- Ensure the workforce has been “appropriately” trained, especially newer staff and that they understand and are effective in protecting privacy
  - Look for failures in:
    - Practical Realities
    - Human Error
    - Limited staff time
    - Limited Resources

---

---

---

---

---

---

---

---

**FOCUS for OCR Audits - Measuring impact on your practice**

- Staff Awareness of HIPAA privacy and security regulations
- Staff Know how and where PHI is created, received, stored and transmitted
- Staff Trained regarding breach notification requirements
- Follow up regarding stated action for mitigation
- Policy and Procedures versus actual Practice

---

---

---

---

---

---

---

---

**OCR - provided a HIPAA security risk assessment tool**

- The tool will greatly assist providers in performing a risk assessment (SRA) to meet their obligations under the HIPAA Security Rule
- <http://www.healthit.gov/security-risk-assessment> Developed by using National Institute of Standards and Technology (NIST) and Security Content Automation Protocol (SCAP) <http://scap.nist.gov/hipaa/>
- The SRA tool and its additional resources have been designed to help health care providers conduct a risk assessment to support better privacy and security for patient health data
- The SRA tool is a core requirement for eligible providers and hospitals seeking payment through the Meaningful Use Program

---

---

---

---

---

---

---

---


**Practical steps for Information Release Compliance**

Revising intake and patient management workflows

Creating new operational checklists

Assessing and modifying practice management/EMR/E-HR systems

Complying with Omnibus while also supporting complete documentation and continuity of care




---

---

---

---

---

---

---

---

---

---

**Updated Meaningful Use Timeline**

First Payment Year	Stage of Meaningful Use											
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	
2011	1	1	1	2*	2	3	3	TBD	TBD	TBD	TBD	
2012		1	1	2*	2	3	3	TBD	TBD	TBD	TBD	
2013			1	1*	2	2	3	3	TBD	TBD	TBD	
2014				1*	1	2	2	3	3	TBD	TBD	
2015					1	1	2	2	3	3	TBD	
2016						1	1	2	2	3	3	
2017							1	1	2	2	3	

\*3-month quarter EHR reporting period for Medicare and continuous 90-day EHR reporting period (or 3 months at state option) for Medicaid EPs. All providers in their first year in 2014 use any continuous 90-day EHR reporting period.

---

---

---

---

---

---

---

---

---

---

**Where am I and What Should I Do???**

If you were scheduled to demonstrate:	You would be able to attest for Meaningful Use:		
	Using 2011 Edition CEHRT to do:	Using 2011 & 2014 Edition CEHRT to do:	Using 2014 Edition CEHRT to do:
Stage 1 in 2014	2013 Stage 1 objectives and measures*	2013 Stage 1 objectives and measures* -OR- 2014 Stage 1 objectives and measures*	2014 Stage 1 objectives and measures
Stage 2 in 2014	2013 Stage 1 objectives and measures*	2013 Stage 1 objectives and measures* -OR- 2014 Stage 1 objectives and measures* -OR- Stage 2 objectives and measures*	2014 Stage 1 objectives and measures* -OR- Stage 2 objectives and measures

\*Only providers that could not fully implement 2014 Edition CEHRT for the EHR reporting period in 2014 due to delays in 2014 Edition CEHRT availability.

---

---

---

---

---

---

---

---

---

---

**Meaningful Use Stage 2**

- **Hardship Exemption**
  - "Significant hardship"
  - If granted, valid for one year
  - To qualify, have to demonstrate:
    - Lack of infrastructure
    - Unforeseen/uncontrollable circumstances
    - Lack of control over EHR availability
    - Insufficient face-to-face interactions
  - 2014 Application:
    - [http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/HardshipExemption\\_EP\\_Application.pdf](http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/HardshipExemption_EP_Application.pdf)

---

---

---

---

---

---

---

---

**Stage 2 Objectives**

- **EP: 17 Core, 3 Menu**
- **H: 16 Core, 3 Menu**
  
- **New core objectives highlights:**
  - Secure messaging for patients
  - Track medications electronically
  - Patient access objectives
  - Patient transmit health information within 4 days (36 hours post hospital discharge)
  - Coordination of Care: electronic summary for referred patients (at least 10%)

---

---

---

---

---

---

---

---

**Stage 2 Menu Items**

- **New Menu Selections:**
  - Record notes electronically in patient records
  - Imaging results available through CEHRT
  - Record patient family health history
  - Identify and report to other registries
  - Identify and report cancer cases to cancer registry

---

---

---

---

---

---

---

---



**Stage 2 CQMs**

- **Must report 9 of 64 CQMs**
- **All providers should report on 3 of 6 health care policy domains (i.e...)**
  - Patient and Family Engagement
  - Patient Safety
  - Care Coordination
  - Clinical Processes/Effectiveness

**REPORT ONLY TO CMS... NO BASELINES**

---

---

---

---

---

---

---

---

**Core Objectives for Stage 2 Related to Patient Portals**

- **EP:**
  - Provide patients the ability to VDT their health information online within 4 business days of the information being available to the EP
  - Use secure electronic messaging to communicate with patients on relevant health information
- **Hospital:**
  - Provide patients the ability to VDT information about a hospital admission

---

---

---

---

---

---

---

---

**Issues to Resolve before VDT Access Granted**

- **Is the person authorized to access PHI through VDT, either due to authorization from the patient or due to legal status?**
- **Identification and authentication of the individual or entity granted access (are they who they say they are?)**
- **Education of patient and providers on rights, responsibilities, and limitations is key**
  - ADDRESS RISKS OF "VIEW"
  - ADDRESS RISKS OF "DOWNLOAD"
  - Things for you to think about:
    - Minimize or avoid repeat notices
    - Ensure no cache copies retained
    - Automatically terminate session after period of time

---

---

---

---

---

---

---

---

**Privacy**

- Identify proofing and authentication
- Patients may accomplish VDT access on their own by sharing user names and passwords.
  - Not advisable
- 2 factor authentication to access portals is highly encouraged
- Authentication of user trying to access information (i.e. out-of-band confirmation)
- Process to cut off VDT access by friends, family and personal representatives due to patient change in preferences or changes in personal representative legal status
- Role based access for i.e. personal representatives, etc.?

---

---

---

---

---

---

---

---

**Principles**

- Protections should be commensurate with risks
- Approaches should offer simplicity and ease of use for patients and be consistent with what patients are willing and able to do.
- Solutions should provide flexibility in the methods offered; "ONE SIZE DOES NOT FIT ALL."
- Approaches should leverage solutions in other sectors, such as online banking
- Solutions should be accompanied by education that make these processes transparent to the patient.
- Approaches taken should build to scalable solutions (i.e. greater use of voluntary secure identity providers such as those envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC))
- Solutions need to evolve over time as technology changes

---

---

---

---

---

---

---

---

**Gaining Consent**

- Registrars hold the keys to patient engagement with the HIE
- Several Ways HIM Can Help
  - 1) Educate registrars about the benefits of portals & HIEs and how they operate
  - 2) Create portal and HIE Scripts
  - 3) Underscore the importance of meaningful consent
  - 4) Encourage Registrars to promote the patient portal
  - 5) Alter the registration process
  - 6) Involve Patient Access in a multi-media approach



---

---

---

---

---

---

---

---

**Sharing Patient Information in an Exchange**

- **Why HIE matters to physician practices**
  - Longitudinal record
  - Triple AIM
- **Establishing stronger collaboration partnerships through information exchange**

---

---

---

---

---

---

---

---

**HIM's Role with HIEs**

- **Data Governance**
- **MPI / EMPI**
- **HIPAA & HITECH requirements**
- **Policies & Procedures**
- **State & Federal Requirements for Confidentiality**
- **Breach Notification Requirements**
- **Integration of Data Elements**
- **Best Practices in Information Management**

---

---

---

---

---

---

---

---

**Best practices for safe information sharing within an HIE: Information Governance**

- |  |   |
|--|---|
| *Data Conversion Planning Policy                       | *Electronic Record Linking Policy                       |
| *Enterprise Data Integrity Maintenance Policy          | *Maintenance of user and Provider Master Records Policy |
| *Policy on an Integrated Medical Record                | *Patient Involvement in Medical Record Accuracy Policy  |
| *Core Patient Identifiers and Naming Convention Policy | *Legal Medical Record & eDiscovery                      |
| *Medical Record Corrections Policy                     | *Data Ownership & DURSA Agreements                      |
| *Duplicate Record Validity Determination Policy        | *HIE Opt in / Opt Out                                   |
| *Record Search Policy                                  | *Red Flag Alert   |
| *Data Conversion Testing Policy                        | *Data Governance Terms and Definitions                  |

---

---

---

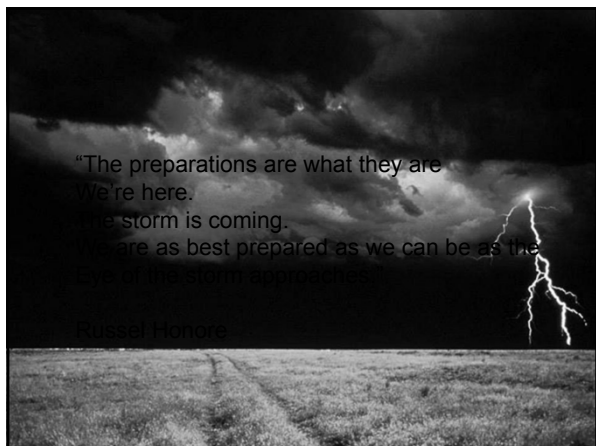
---

---

---

---

---



---

---

---

---

---

---

---

---

**Conclusions - Audit Findings**

- 800+ major health data breaches in last 4 years
- Entity wide Controls
- Access Controls
- Network Operations Controls

---

---

---

---

---

---

---

---

**Largest HIPAA Settlements**

- Joint settlement by New York-Presbyterian Hospital and Columbia University (April 2014)
  - Combined \$4.8 million settlement was the largest payout of any kind to settle a HIPAA case
  - 6,800 patient records exposed to the Internet \$706.00 per record
    - New York-Presbyterian, whose computer server was exposed to the Internet, paid \$3.3 million
    - Columbia University, whose employed physician worked with the network that exposed the patient data, paid \$1.5 million
    - Columbia University employee accessed information from New York-Presbyterian for research purposes... no fine imposed

---

---

---

---

---

---

---

---

**Largest HIPAA Settlements – by records exposed**

- 2011 settlement with Massachusetts General Hospital for \$1 million
  - Employee in 2009 left 193 paper records of infectious-disease patients, including patient with HIV, on a computer train
  - Cost-per-record basis of \$5,208 each
  
- Civil monetary penalty, only one issues so far in a HIPAA case
  - Resulted from not providing 41 individuals access to their medical records, and went to Cignet Health at \$4.3 million
  - Eventually raised to just short of \$4.8 million, after litigation

---

---

---

---

---

---

---

---

**Health Companies Settle HIPAA Allegations**

- Two Health-care companies agreed to pay civil penalties to resolve allegations they violated HIPAA rules on securing electronic protected health information (OCR, April 22, 2014)
  - Both stemmed from the theft of unencrypted laptops
- Largest of two settlements involved Concentra Health Services – will pay \$1.7 million to OCR and adopt a corrective action plan to address alleged violations that included failing to encrypted laptops, desktop computers, medical equipment, tablet computers and other devices with e-PHI
- OCR did a compliance review following a data breach report involving theft of unencrypted laptop from a Concentra physical therapy center
  - Found that Concentra had identified the lack of encryption on its computing and other devices as a “critical risk”, but failed to fully address the issue
  - “insufficient security management processes in place to safeguard patient information.”

---

---

---

---

---

---

---

---

**HIPAA Enforcement**

- Predictions that HIPAA enforcement will expand significantly
  - Because of obligation to report breaches, expect that OCR will have numerous opportunities with which to conduct investigations
- In addition, state attorneys general (AG) remain an important wild card
  - Despite having broad general authority on consumer protection, specific authority in many states under data breach notification laws and explicit new authority to enforce the HIPAA rules, AG enforcement have been noticeably and surprisingly absent in connection with their HIPAA/HITECH authority
- Omnibus – proposal for “whistle blowing” and sharing of resulting findings with individuals who report privacy and security concerns

---

---

---

---

---

---

---

---

Sometimes its wise to warn  
even about obvious risks



Don't drive off the dock



---

---

---

---

---

---

---

---



"Look for me in the whirlwind or  
the storm" (Marcus Garvey)

[Rita.Bowen@healthport.com](mailto:Rita.Bowen@healthport.com)

[Alisha.Smith@healthport.com](mailto:Alisha.Smith@healthport.com)

---

---

---

---

---

---

---

---