HIPAA Survival in 2016 and Beyond

Presented by: Susan Clarke, HCISPP, HTS Department Manager, and Steve Marco, President and Founder HIPAA One
March 23, 2016 – 1–2 PM MDT
Welcome

- Thank you for spending your valuable time with us today.
- This webinar will be recorded for your convenience.
- A copy of today’s presentation and the webinar recording will be available on our website. A link to these resources will be emailed to you following the webinar.
- All phones will be muted during the presentation and unmuted during the Q&A session. Computer users can use the chat box to ask questions which will be answered at the end of the presentation.
- We would greatly appreciate your providing us feedback by completing the survey at the end of the webinar today.

HTS, a department of MPQHF, has assisted 1480 providers and 50 Critical Access Hospitals to reach Meaningful Use. We also assist healthcare facilities with utilizing Health Information Technology (HIT) to improve health care, quality, efficiency and outcomes.
• HealthInsight holds the Centers for Medicare & Medicaid Services (CMS) Quality Innovation Network Quality Improvement Organization (QIN–QIO) contract for Nevada, New Mexico, Oregon and Utah; and also holds the CMS end-stage renal disease (ESRD) contract for Networks 16 and 18, serving Alaska, Idaho, Montana, Oregon, Washington and Southern California.

• As a Regional Extension Center (REC), HealthInsight has assisted 1,976 providers and 30 critical access hospitals in Nevada and Utah adopt electronic health record (EHR) technology. The REC also assisted more than 1,400 providers in meeting Meaningful Use Stage 1.
- HIPAA Compliance & Information Security
  - Superior Technology and Service
  - Client and Partner Support

- HIPAA One® Risk analysis software:
  - Over 1,600 sites (CEs and BAs)
  - Automation of all mundane, error-prone and labor-intensive activities
  - Roadmap includes Privacy and BAA

- Developed and maintained in USA
  - SOC2, Security and Compliance
Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)’ opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users individual needs.
Session Presenters

- Susan Clarke, HCISPP
- Steven Marco, CISA
- P.A.T.
Agenda

Attack surfaces getting attention – 5 mins

HIPAA and Compliance – 10 mins

Audits and Breaches – 10 mins

SRA Acceleration using HIPAA One® – 20 mins

Contact and Q&A – open
Today, Health Technology has become an integral component of providing health care delivery.

We are becoming dependent on technology that is growing faster than our ability to secure it...

This technology extends to systems that can affect public safety and human life.
EMR support to help us achieve the Triple Aim

- **Availability**
  - Access to electronic chart

- **Confidentiality**
  - Electronic chart is private

- **Integrity**
  - Trust the electronic chart

**Per Capita Cost**

**Population Health**

**Experience of Care**

*Triple Aim source: Institute for Healthcare Improvement*
Every device with IP is an attack surface

Medical devices increasingly rely upon computers, software, and networking. They often incorporate third-party software and are subject to regulation, which can impact the ability for patch management. They undergo limited clinical trials and are often developed without secure development techniques.
Securing Medical Devices

- Only by working together—medical device manufacturers, hospitals, and regulators—can we ensure our hospitals remain safe.
- The FDA is working hard to raise awareness of the issue.
- Contracts should have specific language to address the detection, remediation and document standard process to remediate and rebuild devices when malware and cyber attackers are using these devices.
- This is a very complex and rapidly evolving ecosystem—securely designed medical device submitted to the FDA for approval today will not see the inside of a hospital (or the inside of a patient) until the 2020s.

Remember the device we make safer today, may be in you tomorrow.
History of HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health). In January of 2013, the Department of Health and Human Services issued a ruling known the Omnibus final rule. The deadline for compliance was September 23, 2013.

HIPAA Rules = Privacy + Security + Breach Notification
“The following entities must follow The Health Insurance Portability and Accountability Act (HIPAA) regulations. The law refers to these as “covered entities”: Health plans. Most health care providers, including doctors, clinics, hospitals, nursing homes, and pharmacies. Jan 15, 2013”
Privacy Rule

- Establishes national standards to protect PHI.
- Applies to **any form of PHI**
- Sets forth requirements to ensure patients’ information stays private
- Patient rights
- Privacy Rule is located at 45 CFR [Part 160](#) and Subparts A and E of [Part 164](#)

Security Rule

- Establishes national standards to protect individuals’ ePHI.
- Apply to **only electronic form** of PHI (ePHI)
- Goal to ensure confidentiality, integrity and availability—CIA triad
- Outlines security safeguards.
- The Security Rule is located at 45 CFR [Part 160](#) and Subparts A and C of [Part 164](#)
**Privacy Officer:** Is responsible for reviewing organization practice and procedures to ensure the compliance with the relevant privacy laws & policies. The privacy officer will be able to make recommendations to prevent incidents of compromise & misuse of health or personal information.

**Security Officer:** Is responsible for the design, implementation, management & review of the org's security policies, standards, procedures, baselines & guidelines. Directs, coordinates & organizes information security activities throughout the organization.
The Breach Notification Rule:

What to Do If You Have a Breach?

“A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. An impermissible use or disclosure of unsecured PHI is presumed to be a breach unless the CE or BA demonstrates (based on a risk assessment) that there is a low probability that the PHI has been compromised.”

If in doubt seek a qualified attorney specializing in HIPAA Compliance.

Do you know where all your PHI and ePHI is located?

Chain of Trust

Covered Entity

Business Associate

Subcontractor

Subcontractor
Business Associate

What Is a “Business Associate?” A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. The Privacy Rule requires you obtain satisfactory assurances the BA will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.

Today’s challenges:
- BA security questionnaires may not get returned or sometimes returned incomplete
- May be working on the honor system when proof is required
- May refuse to provide reasonable assurances of HIPAA compliance other than signed BAA
Your contracts should include:

- Service provider/vendor must perform risk assessments that meet National Institute of Standards and Technology (NIST) Special Publication 800–30.
- Must provide annual copy of risk assessment.
- Service provider is liable for damages if fails to properly perform a risk assessment.

This gives you an addition layer of protection, contract rights and Business Associate provisions.
Yes, Healthcare is being targeted.
Clinical teams manage risk on a daily basis yet security risk management programs are often not as formal as needed.

Organizations need to understand probability over the cost of safeguard and make informed decisions. All systems contain flaws – technology systems are no different.
Culture of Compliance

Strong commitment, visible and explicit in rewards, punishment and requirements. Compliance team has direct line to top, adequate funding and resources to do their job.
Effective Compliance Program

- Have written policies and standards of conduct.
- Designated Compliance Officer.
- Effective training and education.
- Effective lines of communication.
- Enforcement of standards through disciplinary guidelines (publicized & enforced).
- Internal monitoring and auditing.
- Response and corrective action plan for offenses.
- Conduct regular risk assessments.
HIPPOs and HIPAA
There are 5 ways to get audited:

1. **Patient Complaint/Whistleblower**
   - Privacy (PHI), Security (ePHI) or possible Breach Notice

2. **Breach Notice**
   - Omnibus update: all unauthorized disclosures are breaches

3. **Meaningful Use**
   - Core Measure regarding “Protecting ePHI”

4. **Random Audit**
   - Newman Research, Audit Protocol, ongoing audits

5. **Business Associates**
   - Regardless “who’s fault” the CE is responsible
How to Prepare For An Audit?

- Perform a comprehensive HIPAA Security Risk Analysis
- React: Implement plans to remediate deficiencies
- Understand HIPAA Compliance vs Security
  - **HIPAA Security** is the effort to safeguard ePHI to preserve confidentiality, availability and integrity of the data
  - **HIPAA Compliance** is the act proving the organization’s intent to meet the requirements of the HIPAA Security Rule
- OCR’s Final Guidance on Risk Analysis:
**Must We Outsource the SRA?**

**Source:** HHS Privacy and Security Guide of Health Information, page 6:

As with any new program or regulation, there may be misinformation making the rounds. The following table distinguishes fact from fiction.

<table>
<thead>
<tr>
<th>Myth</th>
<th>Fact</th>
</tr>
</thead>
<tbody>
<tr>
<td>The security risk analysis is optional for small providers.</td>
<td>False. All providers who are “covered entities” under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.</td>
</tr>
<tr>
<td>Simply installing a certified EHR fulfills the security risk analysis MU requirement.</td>
<td>False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.</td>
</tr>
<tr>
<td>My EHR vendor took care of everything I need to do about privacy and security.</td>
<td>False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.</td>
</tr>
<tr>
<td>I have to outsource the security risk analysis.</td>
<td>False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.</td>
</tr>
</tbody>
</table>
Is Updating Risk Progress Enough?

<table>
<thead>
<tr>
<th>Before I attest for an EHR incentive program, I must fully mitigate all risks.</th>
<th>False. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each year, I’ll have to completely redo my security risk analysis.</td>
<td>False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks. Under the Meaningful Use Programs, reviews are required for each EHR reporting period. For EPs, the EHR reporting period will be 90 days or a full calendar year, depending on the EP’s year of participation in the program.</td>
</tr>
</tbody>
</table>

To learn more, visit the Privacy and Security Resources page for more information.

Guide to Privacy and Security of Health Information

Updating last year’s remediation plan is **NOT** the same as **AUDITING CHANGES AND RISKS** since last year…
In a Breach, Who pays?

- **Covered Entities (CE)**
  - § 160.402(c)(1) “A covered entity is liable...for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.”

- **Business Associates (BA)**
  - § 160.402(c)(2) “A business associate is liable...for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.”
Free Risk Assessment Tools

- HHS and REC Spreadsheets – Excel is amazing!
  - Process is ambiguous, easy to lose and doesn’t always pass.
Free Risk Assessment Tools

- SRAT – New and improved (2014)
  - Manual, still no collaboration, software updates or support

- Can you determine likelihood and impact?
Risk Assessment Tools

- SRAT – doesn’t guarantee or assure compliance...

![Risk Assessment Tool](image)
How is a HIPAA SRA done?

Input
- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

- History of system attacks
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media.

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

- Current controls
- Planned controls

Risk Assessment Activities

Step 1. System Characterization

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 2. Threat Identification

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 3. Vulnerability Identification

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 4. Control Analysis

Step 5. Likelihood Determination

Step 6. Impact Analysis

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Step 7. Risk Determination

Step 8. Control Recommendations

Step 9. Results Documentation

Output

- System boundary
- System functions
- System and data criticality
- System and data sensitivity

- Threat statement

- List of potential vulnerabilities

- List of current and planned controls

- Likelihood rating

- Impact rating

- Risks and associated risk levels

- Recommended controls

- Risk assessment report

- Fully Automated

HIPAAOne®
PROTECT YOUR ePHI

How is a HIPAA SRA Done using:

Step 1 – Gather Information, Interviews, Inventory, etc.
  ◦ Login, answer simple questions and upload inventory.

Step 2 – Remediation Planning (Onsite)
  ▪ Results of Step 1, Develop and Assign tasks

Step 3 – Completed SRA
  ▪ Ongoing Remediation, tracking and documentation
Are you doing all you can to safeguard your patient’s private health record? Health care data is now a high-value target for hackers, and the cost of a breach goes well beyond the cost of the data loss.

We offer affordable Security Risk Assessment packages using HIPAA One® certified compliant software following the NIST framework.

To learn more please contact:

Susan Clarke,
Health Care Information Security Privacy Practitioner
sclarke@mpqhf.org
307-248-8179
Important Links

Security practices:

Business Associate:
- [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html)

Breach Notification Rule:
Important Links

- Privacy practices:
  http://www.healthit.gov/providers-professionals/model-notices-privacy-practices
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html

- ONC Privacy and Security Guide: