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.

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive Helena, MT 59602•www.healthtechnologyservice.com•406.457.5897
transforming health care through innovative technology

- Mountain-Pacific holds the Centers for Medicare & Medicaid Services (CMS) Quality Innovation Network-Quality Improvement Organization (QIN-QIO) contract for the states of Montana, Wyoming, Alaska and Hawaii, providing quality improvement assistance.

- 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

- 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 One®

PROTECT YOUR ePHI

- **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

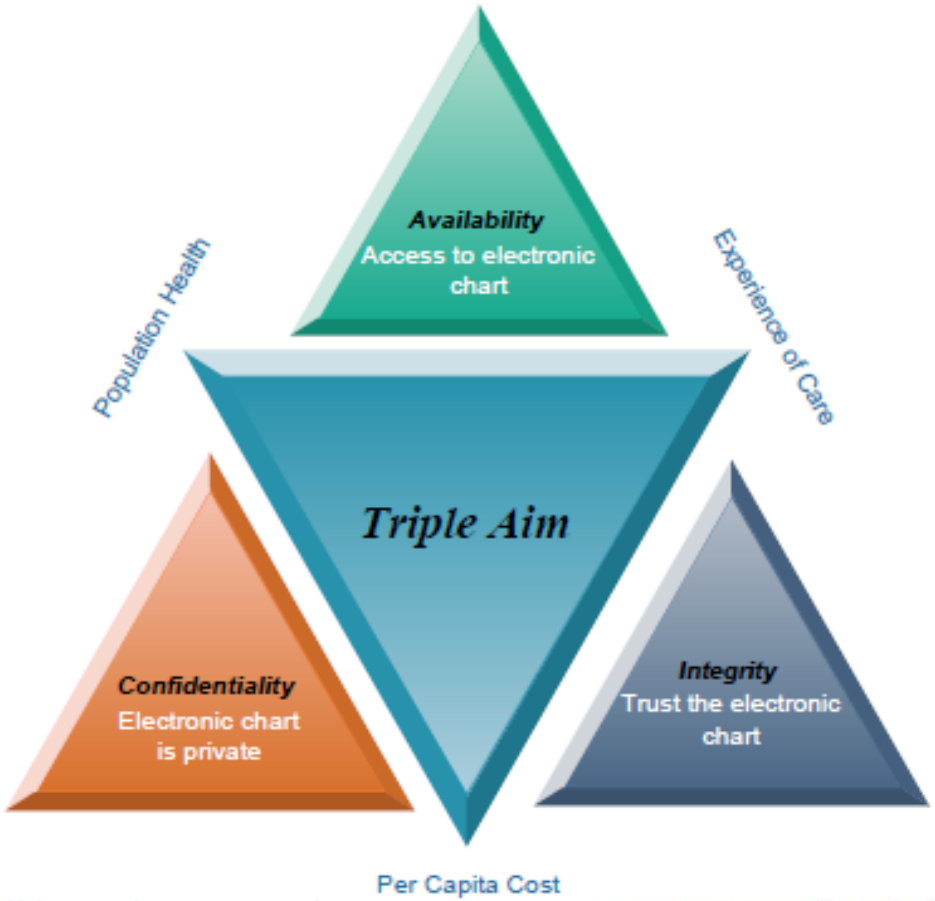
mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive Helena, MT 59602•www.healthtechnologyservice.com•406.457.5897
transforming health care through innovative technology

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



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

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive Helena, MT 59602•www.healthtechnologyservice.com•406.457.5897
transforming health care through innovative technology

Securing Medical Devices

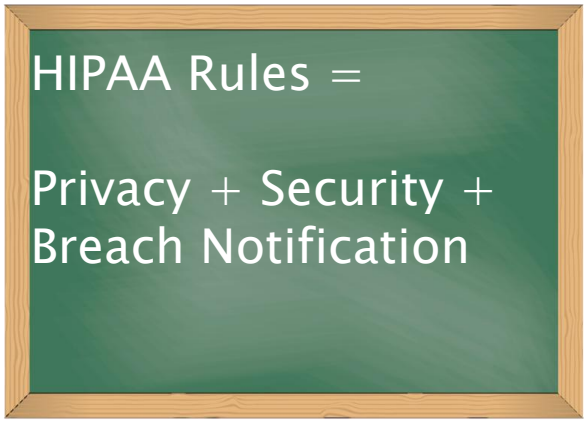
- Only by working together—medical device manufacturers, hospitals, and regulators—can we ensure our hospitals remain safe
- The FDA is working hard to raise awareness of the issue.
- Contracts should have specific language to address the detection, remediation and document standard process to remediate 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 umbrella…

"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

Security Officer

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 orgs security policies, standards, procedures, baselines & guidelines. Directs, coordinates & organizes information security activities throughout the organization.

The Breach Notification Rule:

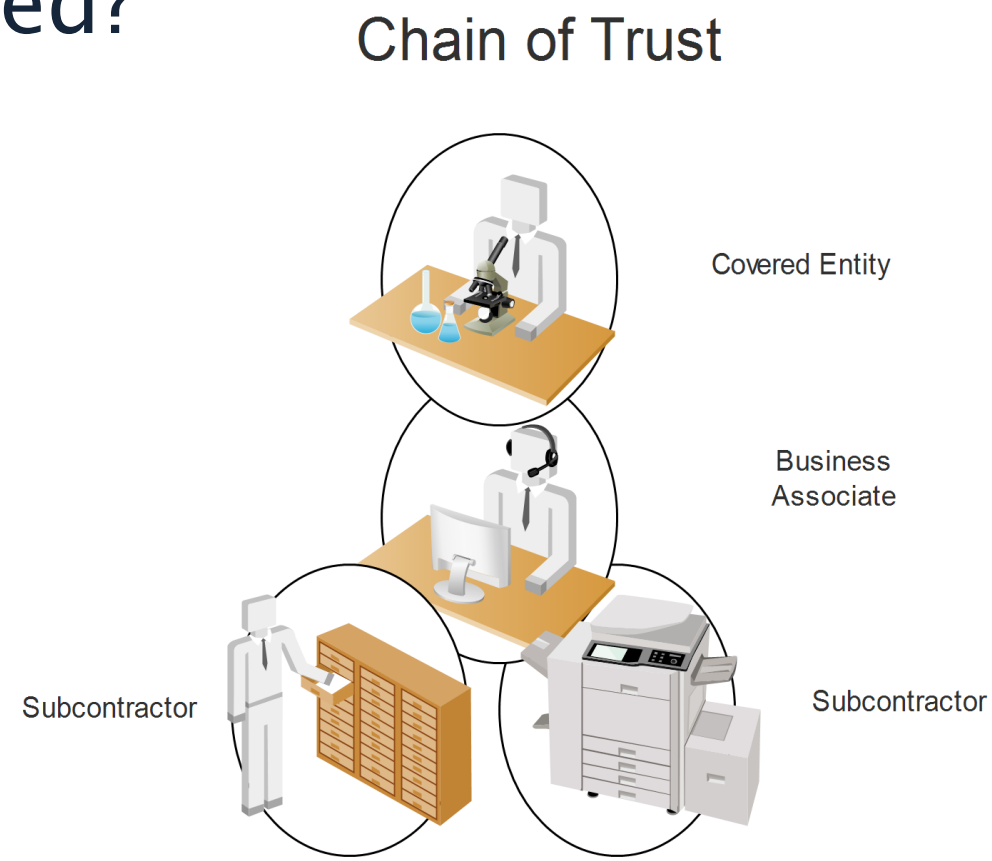
What to Do If You Have a Breach?

"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.

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

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



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

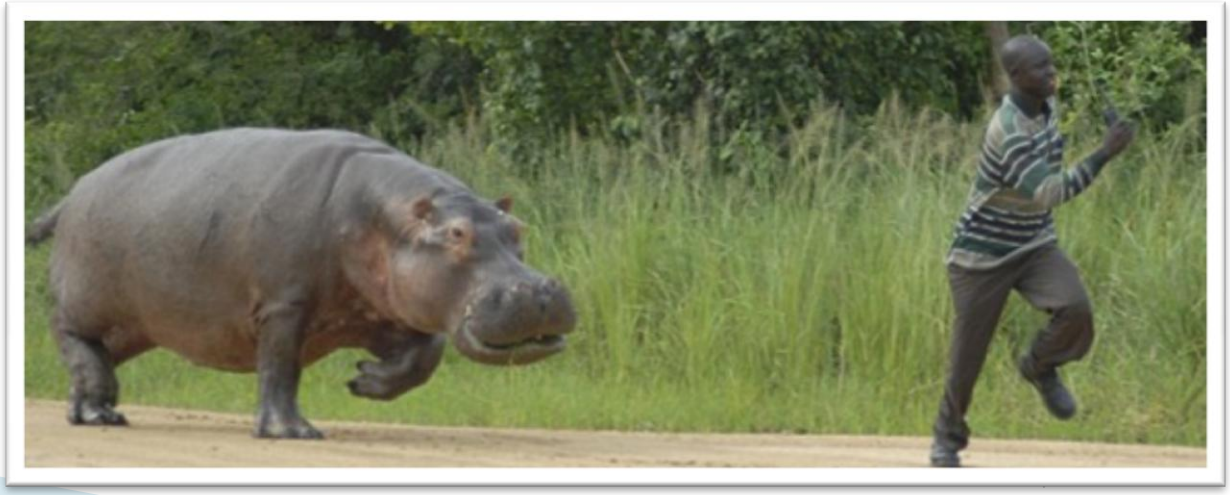
Culture of Compliance

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.

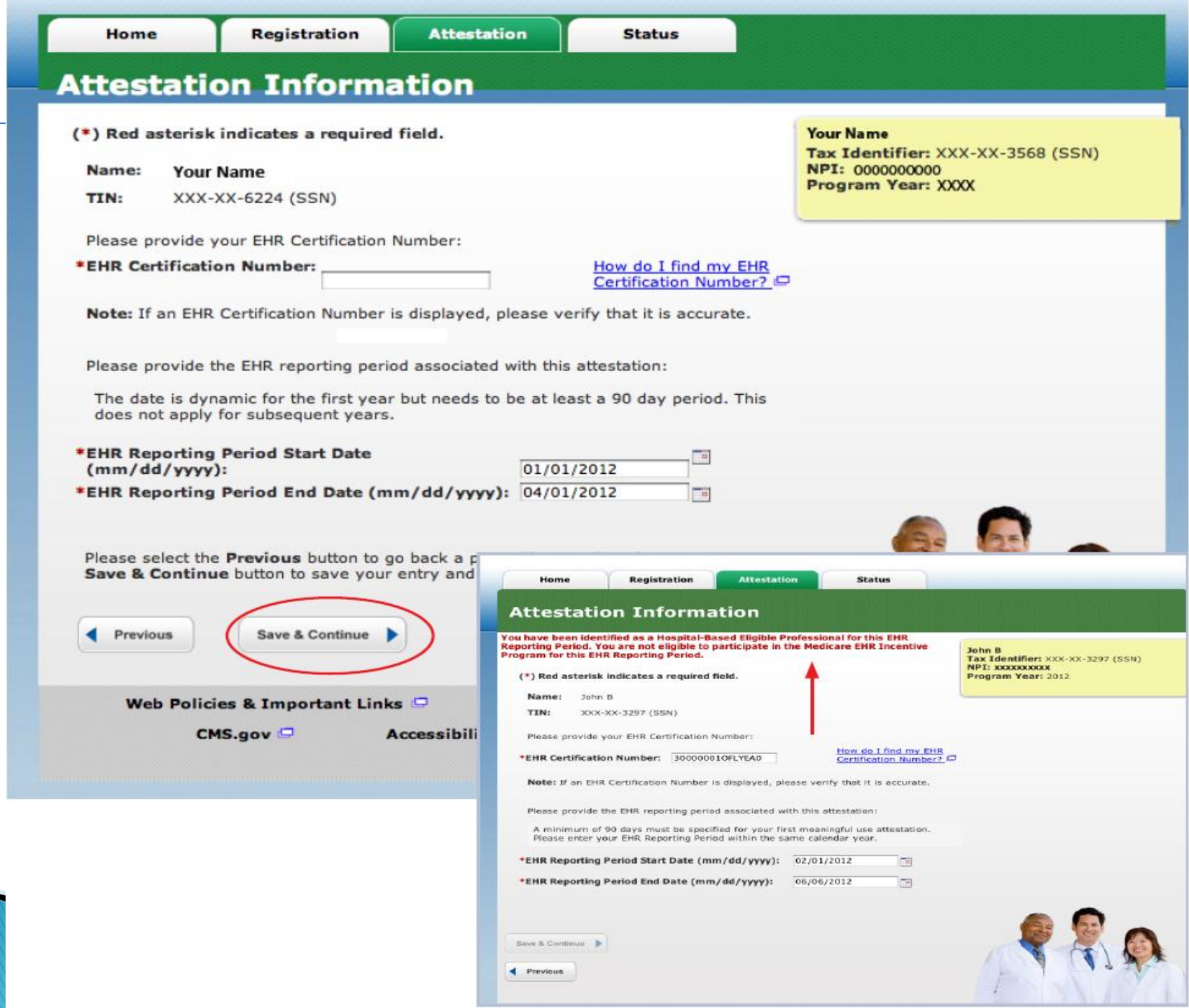
HIPPOs and HIPAA



Problem – High Chance of an Audit

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*


Home
Registration
Attestation
Status
Attestation Information
(*) Red asterisk indicates a required field.
Name: Your Name
TIN: XXX-XX-6224 (SSN)
Your Name
Tax Identifier: XXX-XX-3568 (SSN)
NPI: 0000000000
Program Year: XXXX
Please provide your EHR Certification Number:
*EHR Certification Number:
How do I find my EHR Certification Number?
Note: If an EHR Certification Number is displayed, please verify that it is accurate.
Please provide the EHR reporting period associated with this attestation:
The date is dynamic for the first year but needs to be at least a 90 day period. This does not apply for subsequent years.
*EHR Reporting Period Start Date (mm/dd/yyyy): 01/01/2012
*EHR Reporting Period End Date (mm/dd/yyyy): 04/01/2012
Please select the Previous button to go back a p
Save & Continue button to save your entry and
Previous
Save & Continue
Web Policies & Important Links
CMS.gov
Accessibili
Home
Registration
Attestation
Status
Attestation Information
You have been identified as a Hospital-Based Eligible Professional for this EHR Reporting Period. You are not eligible to participate in the Medicare EHR Incentive Program for this EHR Reporting Period.
John B
Tax Identifier: XXX-XX-3297 (SSN)
NPI: XXXXXXXXX
Program Year: 2012
(*) Red asterisk indicates a required field.
Name: John B
TIN: XXX-XX-3297 (SSN)
Please provide your EHR Certification Number:
*EHR Certification Number: 30000001OFLYEA0
How do I find my EHR Certification Number?
Note: If an EHR Certification Number is displayed, please verify that it is accurate.
Please provide the EHR reporting period associated with this attestation:
A minimum of 90 days must be specified for your first meaningful use attestation. Please enter your EHR Reporting Period within the same calendar year.
*EHR Reporting Period Start Date (mm/dd/yyyy): 02/01/2012
*EHR Reporting Period End Date (mm/dd/yyyy): 06/06/2012
Save & Continue
Previous

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:
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html

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.

Security Risk Analysis Myths and Facts	
Myth	**Fact**
The security risk analysis is optional for small providers.	**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.
Simply installing a certified EHR fulfills the security risk analysis MU requirement.	**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.
My EHR vendor took care of everything I need to do about privacy and security.	**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.
I have to outsource the security risk analysis.	**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.

Is Updating Risk Progress Enough?

Before I attest for an EHR incentive program, I must fully mitigate all risks.	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.
Each year, I'll have to completely redo my security risk analysis.	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.

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

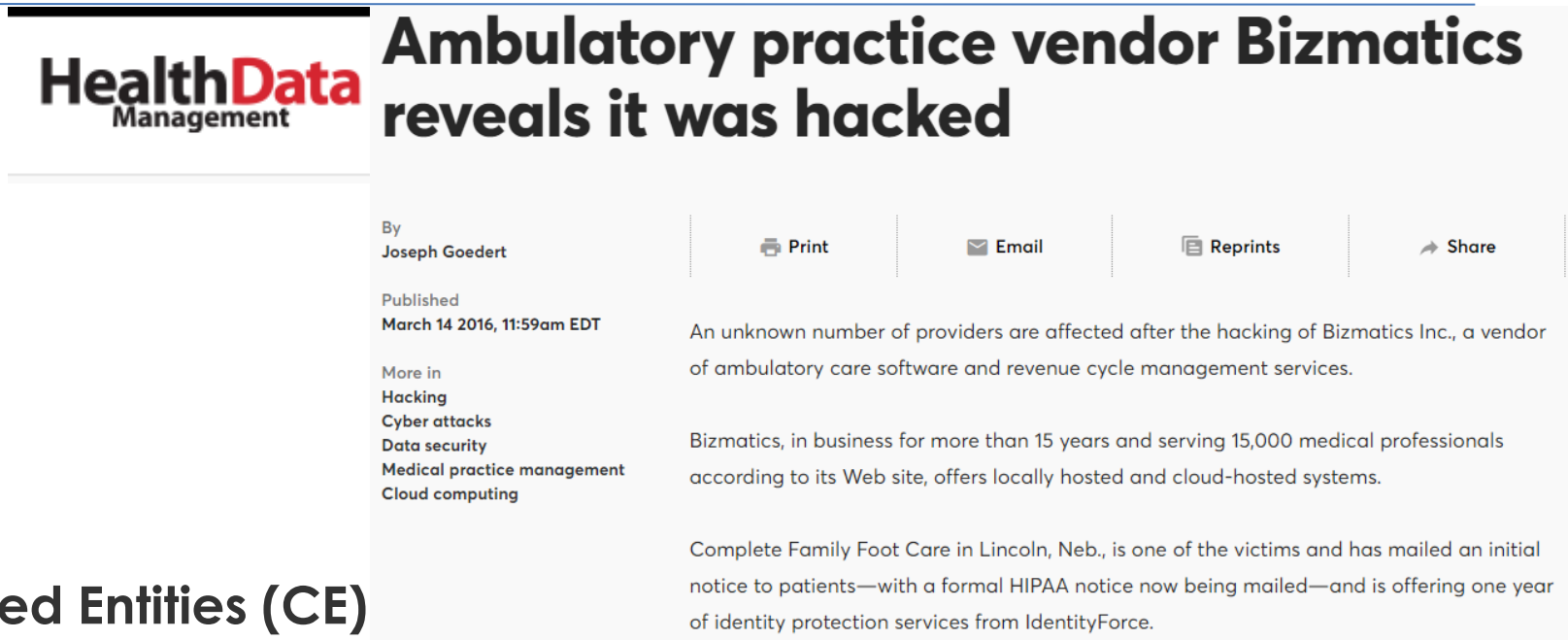
11

Guide to
Privacy and Security
of Health Information

The Office of the National Coordinator for
Health Information Technology

Updating last year's remediation plan is **NOT** the same as **AUDITING CHANGES AND RISKS** since last year…

In a Breach, Who pays?



HealthData Management

Ambulatory practice vendor Bizmatics reveals it was hacked

By
Joseph Goedert

Print | Email | Reprints | Share

Published
March 14 2016, 11:59am EDT

More in
Hacking
Cyber attacks
Data security
Medical practice management
Cloud computing

An unknown number of providers are affected after the hacking of Bizmatics Inc., a vendor of ambulatory care software and revenue cycle management services.

Bizmatics, in business for more than 15 years and serving 15,000 medical professionals according to its Web site, offers locally hosted and cloud-hosted systems.

Complete Family Foot Care in Lincoln, Neb., is one of the victims and has mailed an initial notice to patients—with a formal HIPAA notice now being mailed—and is offering one year of identity protection services from IdentityForce.

- **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."

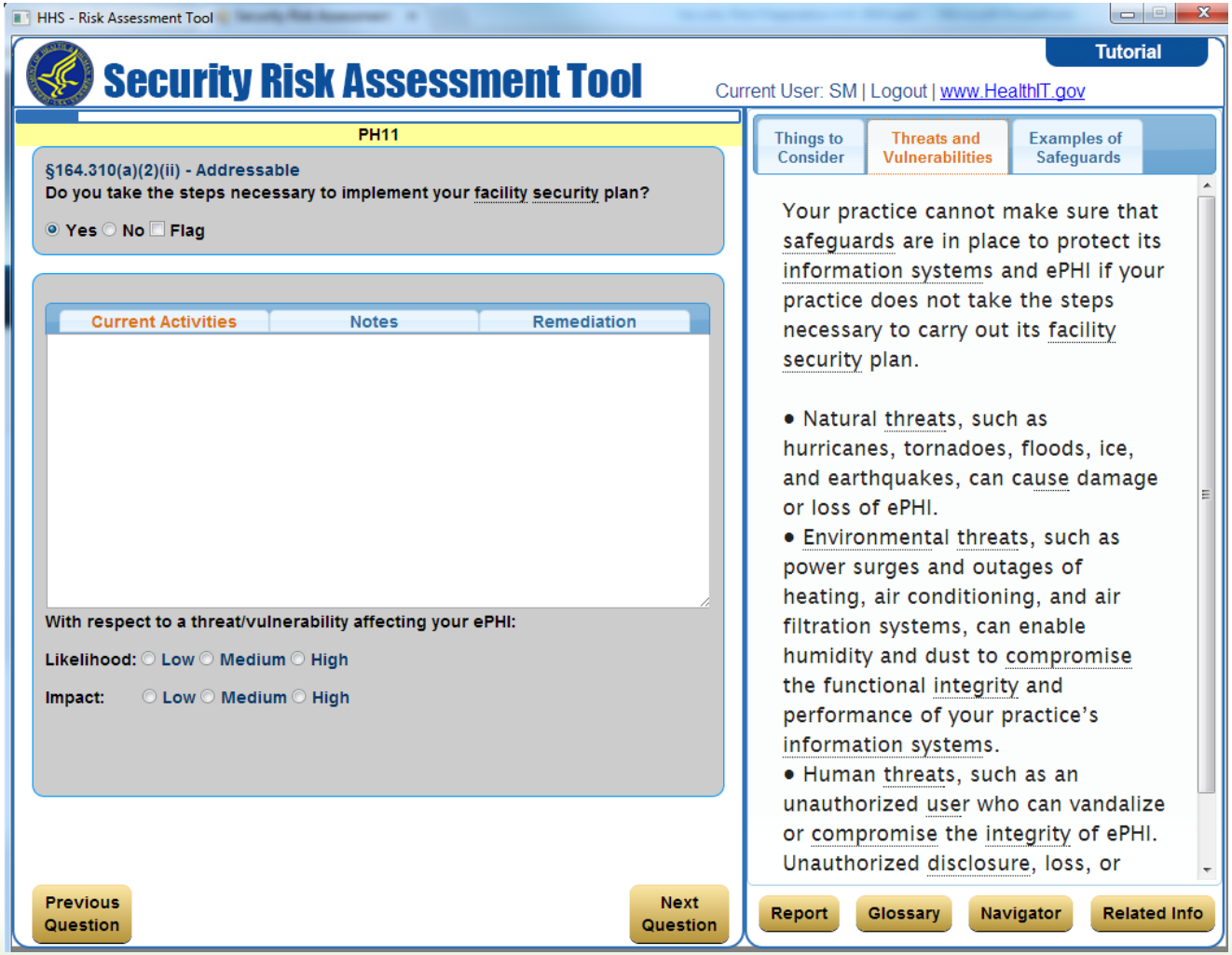
Free Risk Assessment Tools

- HHS and REC Spreadsheets – Excel is amazing!
  - Process is ambiguous, easy to lose and doesn't always pass.

Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Requirement Description	Solution	Compliance Rating Percent	Risk Percent	Planned Start Days	Full Regulatory Text
SECURITY STANDARDS: GENERAL RULES									
1	164.306(a)	**Ensure Confidentiality, Integrity and Availability**	-	Ensure CIA and protect against threats	-	-	-	-	(a) General requirements. Covered entities must
2	164.306(b)	**Flexibility of Approach**	-	Reasonably consider factors in security	-	-	-	-	(b) Flexibility of approach.
3	164.306(c)	**Standards**	-	CEs must comply with standards	-	-	-	-	(c) Standards. A covered entity must comply with
4	164.306(d)	**Implementation Specifications**	-	Required and Addressable Implementation	-	-	-	-	(d) Implementation specifications.
5	164.306(e)	**Maintenance**	-	Ongoing review and modification of security	-	-	-	-	(e) Maintenance. Security measures implemented
ADMINISTRATIVE SAFEGUARDS									
6	164.308(a)(1)(i)	**Security Management Process**	-	P&P to manage security violations	P&P	100	60	90	Implement policies and procedures to prevent,
7	164.308(a)(1)(ii)(A)	Risk Analysis	**Required**	Conduct vulnerability assessment	Assessment	100	60	90	Conduct an accurate and thorough assessment
8	164.308(a)(1)(ii)(B)	Risk Management	**Required**	Implement security measures to reduce risk of	Measures	100	60	90	Implement security measures sufficient to reduce
9	164.308(a)(1)(ii)(C)	Sanction Policy	**Required**	Worker sanction for P&P violations	P&P	100	60	90	Apply appropriate sanctions against workforce
10	164.308(a)(1)(ii)(D)	Information System Activity Review	**Required**	Procedures to review system activity	Procedures	100	60	90	Implement procedures to regularly review
11	164.308(a)(2)	**Assigned Security Responsibility**	-	Identify security official responsible for P&P	Assignment	100	60	90	Identify the security official who is responsible
12	164.308(a)(3)(i)	**Workforce Security**	-	Implement P&P to ensure appropriate PHI access	P&P	100	60	90	Implement policies and procedures to ensure that
13	164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Addressable	Authorization/supervision for PHI access	Procedures	100	60	90	Implement procedures for authorization and/or
14	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Addressable	Procedures to ensure appropriate PHI access	Procedures	100	60	90	Implement procedures to determine that the
15	164.308(a)(3)(ii)(C)	Termination Procedures	Addressable	Procedures to terminate PHI access	Procedures	100	60	90	Implement procedures for termination access to
16	164.308(a)(4)(i)	**Information Access Management**	-	P&P to authorize access to PHI	P&P	100	60	90	Implement policies and procedures for authorizing
17	164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	**Required**	P&P to separate PHI from other operations	P&P	100	60	90	If a health care clearinghouse is part of a larger
18	164.308(a)(4)(ii)(B)	Access Authorization	Addressable	P&P to authorize access to PHI	P&P	100	60	90	Implement policies and procedures for granting
19	164.308(a)(4)(ii)(C)	Access Establishment and Modification	Addressable	P&P to grant access to PHI	P&P	100	60	90	Implement policies and procedures that, based
20	164.308(a)(5)(i)	**Security Awareness Training**	-	Training program for workers and managers	Program	100	60	90	Implement a security awareness and training
21	164.308(a)(5)(ii)(A)	Security Reminders	Addressable	Distribute periodic security updates	Reminders	100	60	90	Periodic security updates.
22	164.308(a)(5)(ii)(B)	Protection from Malicious Software	Addressable	Procedures to guard against malicious software	Procedures	100	60	90	Procedures for guarding against, detecting, and
23	164.308(a)(5)(ii)(C)	Log-in Monitoring	Addressable	Procedures and monitoring of log-in attempts	Procedures	100	60	90	Procedures for monitoring log-in attempts and
24	164.308(a)(5)(ii)(D)	Password Management	Addressable	Procedures for password management	Procedures	100	60	90	Procedures for creating, changing, and
25	164.308(a)(6)(i)	**Security Incident Procedures**	-	P&P to manage security incidents	P&P	100	60	90	Implement policies and procedures to address
26	164.308(a)(6)(ii)	Response and Reporting	**Required**	Mitigate and document security incidents	Measures	100	60	90	Identify and respond to suspected or known
27	164.308(a)(7)(i)	**Contingency Plan**	-	Emergency response P&P	P&P	100	60	90	Establish (and implement as needed) policies and
28	164.308(a)(7)(ii)(A)	Data Backup Plan	**Required**	Data backup planning & procedures	Procedures	100	60	90	Establish and implement procedures to create and
29	164.308(a)(7)(ii)(B)	Disaster Recovery Plan	**Required**	Data recovery planning & procedures	Procedures	100	60	90	Establish (and implement as needed) procedures
30	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	**Required**	Business continuity procedures	Procedures	100	60	90	Establish (and implement as needed) procedures
31	164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Addressable	Contingency planning periodic testing procedures	Procedures	100	60	90	Implement procedures for periodic testing and
32	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	Addressable	Prioritize data and system criticality for	Analysis	100	60	90	Assess the relative criticality of specific
33	164.308(a)(8)	**Evaluation**	-	Periodic security evaluation	Evaluation	100	60	90	Perform a periodic technical and nontechnical
34	164.308(b)(1)	**Business Associate Contracts and Other Arrangemer**	-	CE implement BACs to ensure safeguards	-	100	60	90	A covered entity, in accordance with § 164.306,
35	164.308(b)(4)	Written Contract	**Required**	Implement compliant BACs	Contracts	100	60	90	Document the satisfactory assurances required
PHYSICAL SAFEGUARDS									
36	164.310(a)(1)	**Facility Access Controls**	-	P&P to limit access to systems and facilities	P&P	100	60	90	Implement policies and procedures to limit
37	164.310(a)(2)(i)	Contingency Operations	Addressable	Procedures to support emergency operations and	Procedures	100	60	90	Establish (and implement as needed) procedures

Free Risk Assessment Tools

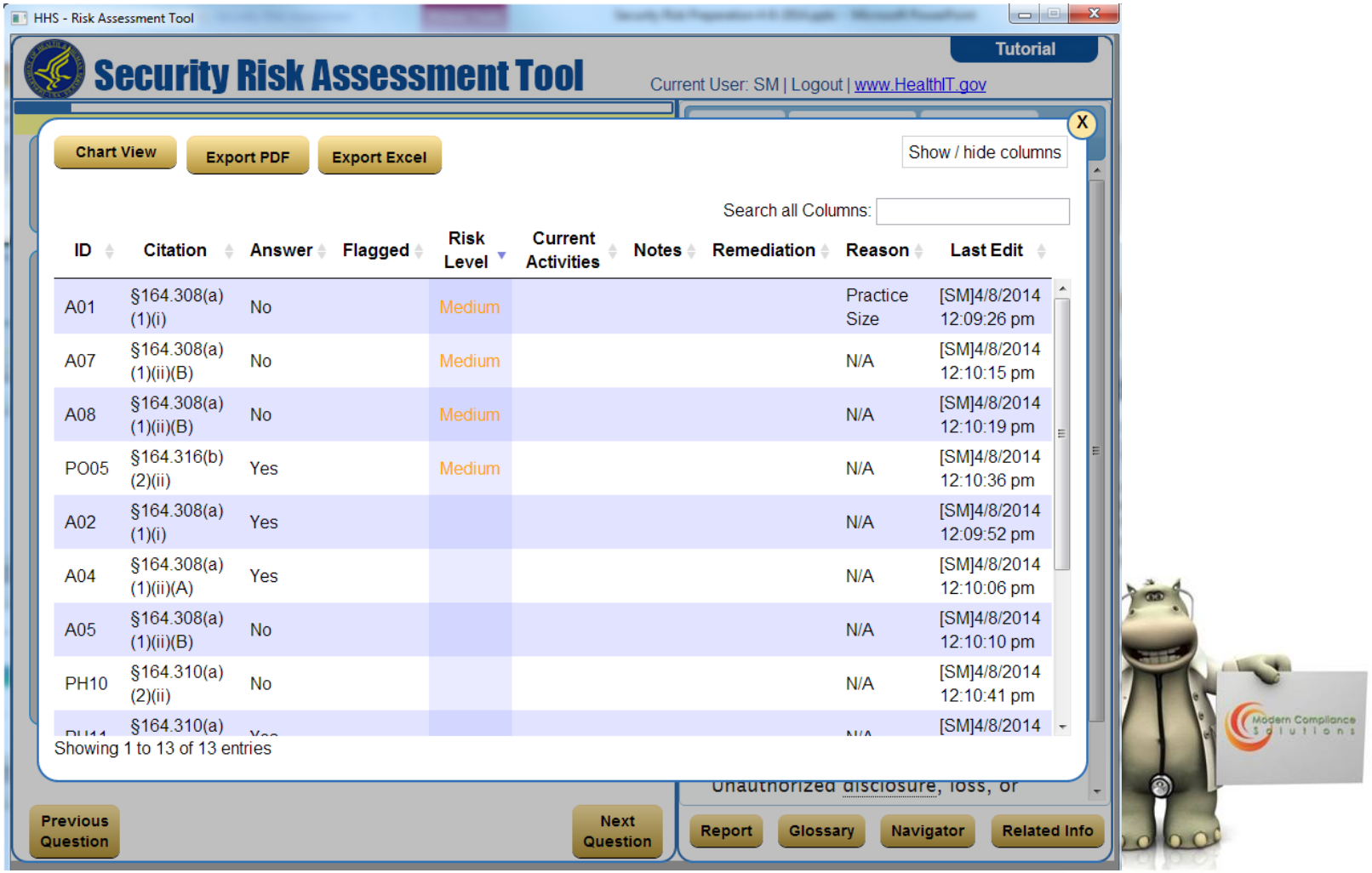
- SRAT – New and improved (2014)
  - Manual, still no collaboration, software updates or support



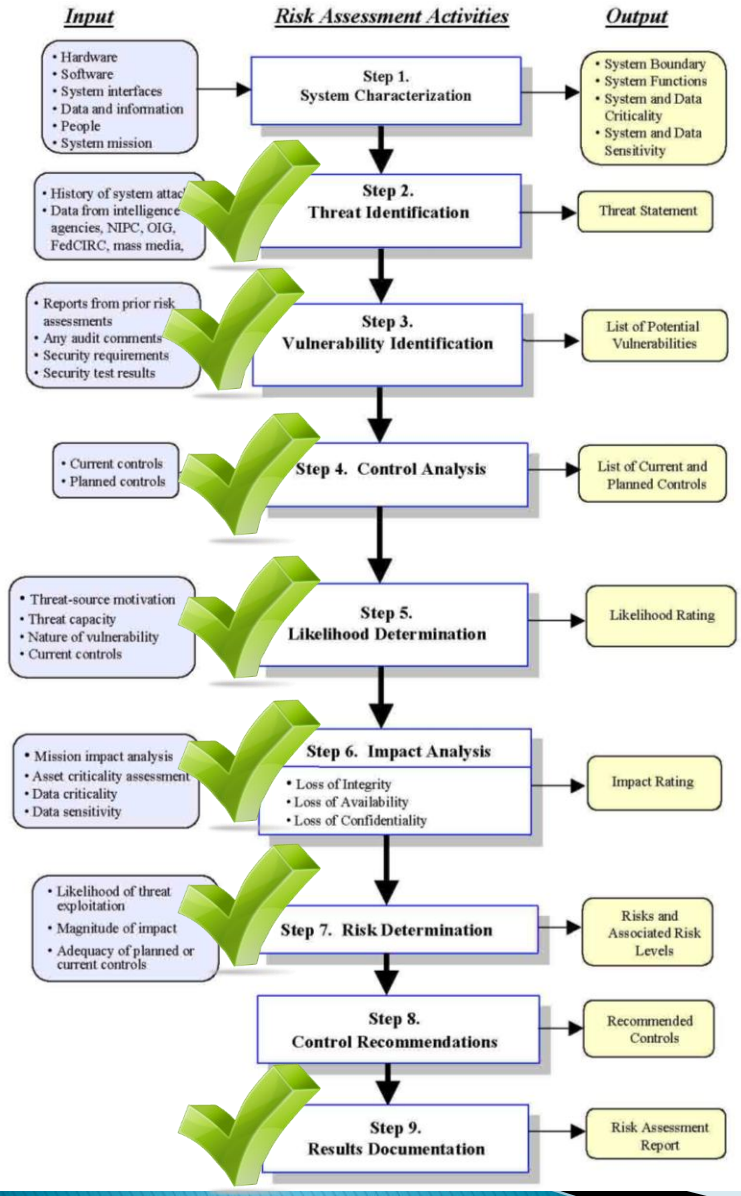
- Can you determine likelihood and impact?

Risk Assessment Tools

- SRAT – doesn't guarantee or assure compliance…



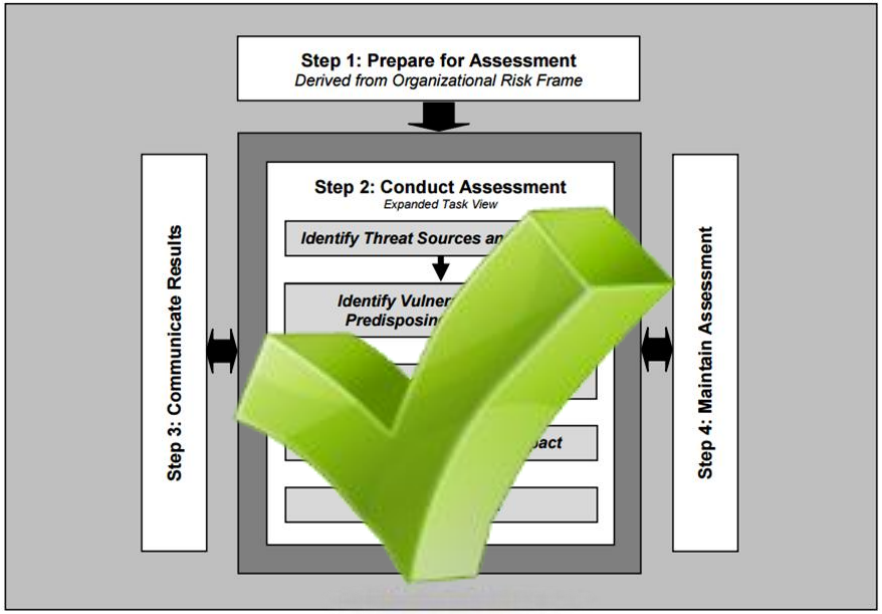
How is a HIPAA SRA done?



- Fully Automated

HIPAAOne®

PROTECT YOUR ePHI



Simple. Automated. Affordable.

How is a HIPAA SRA Done using:

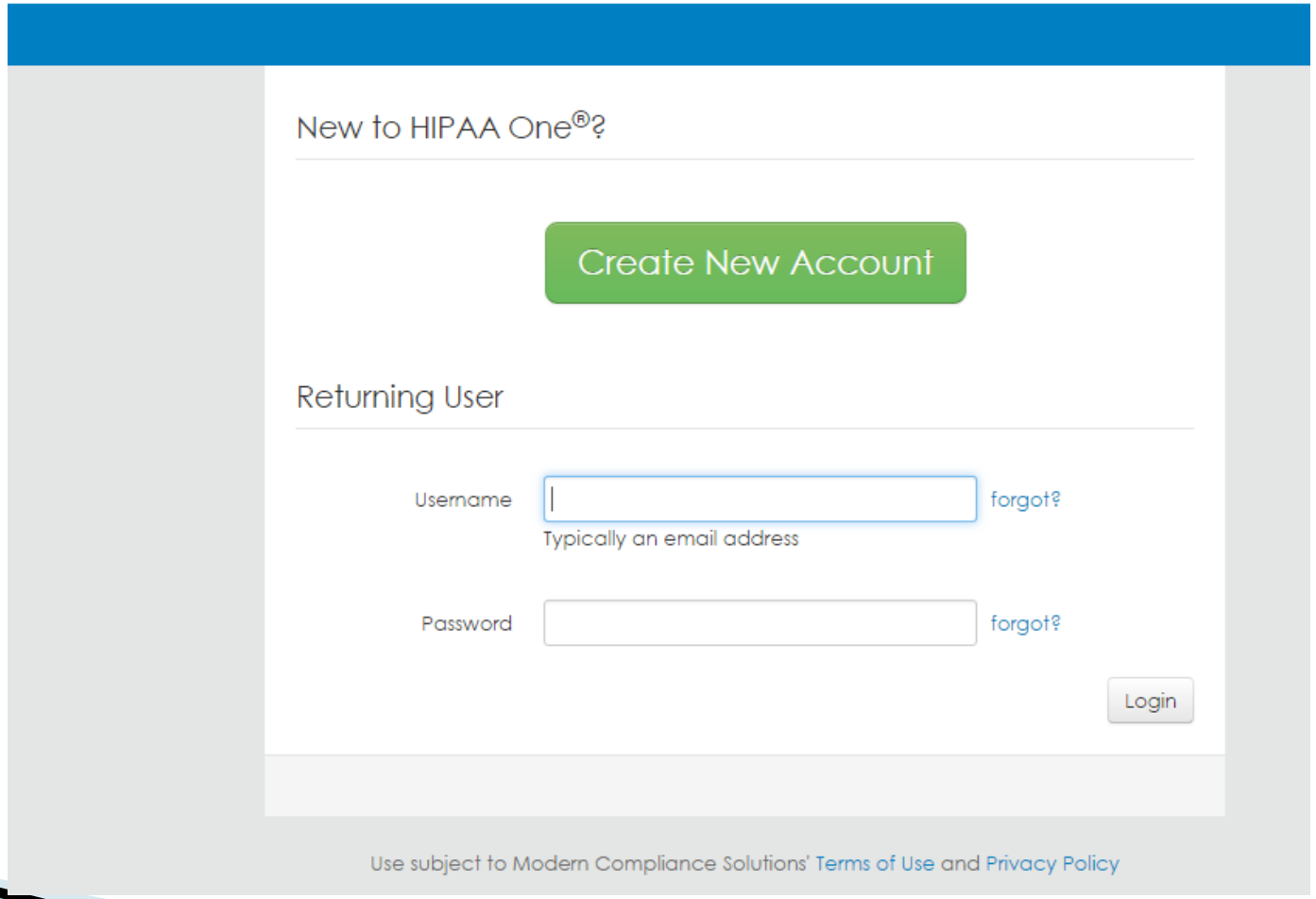
HIPAAOne®
PROTECT YOUR ePHI

- **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**

HIPAA SRA Accelerator



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

Question and Answer

Important Links

Security practices:

- http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Business Associate:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

Breach Notification Rule:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive Helena, MT 59602•www.healthtechnologyservice.com•406.457.5897
transforming health care through innovative technology

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

  http://oncchallenges.ideascale.com/a/pages/digital-privacy-notice-challenge-winners

- ONC Privacy and Security Guide:
  http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pd

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive Helena, MT 59602•www.healthtechnologyservice.com•406.457.5897
transforming health care through innovative technology