Essentials of the Security Risk Analysis 2016

Brett Paepke, OD    Director of ECP Services, Rev360
Jeff Wussow        Business Development Manager, MetaStar
Brad Trudell, JD   HIPAA Privacy & Security Lead, MetaStar

January 20, 2016
Why do you care about a HIPAA compliance?

- RevolutionEHR is a **Business Associate** of your practice and ensures HIPAA compliance regarding how your data is stored, protected and transmitted to you ([http://goo.gl/ejmDkK](http://goo.gl/ejmDkK))

- You are responsible for how data within the practice is protected

- HIPAA requirements have been around longer than Meaningful Use (MU), but MU brought them to the forefront through the Security Risk Analysis requirement
### Meaningful Use Objectives

#### Modified Stage 2
- Protect Patient Health Information
- Clinical Decision Support
- Computerized Provider Order Entry
- Electronic Prescribing
- Health Information Exchange
- Patient Specific Education
- Medication Reconciliation
- Patient Electronic Access
- Secure Electronic Messaging
- Public Health Reporting

#### Stage 3
- Protect Patient Health Information
- Electronic Prescribing
- Clinical Decision Support
- Computerized Provider Order Entry
- Patient Electronic Access to Health Info
- Coordination of Care through Patient Engagement
- Health Information Exchange
- Public Health Reporting

*freedom to focus*
Why do you care about a HIPAA compliance?

- Almost 1300 major data breaches involving the exposure of nearly 135 million individuals' health records since September 2009

Cyberattack Surge: 100M medical records hacked in 2015, officials say

UCLA Health System data breach affects 4.5 million patients

Anthem: Hacked Database Included 78.8 Million People
Health insurer says data breach affected up to 70 million Anthem members

freedom to focus
Why do you care about a HIPAA compliance?

Data Breaches in 2014 by Industry

- Healthcare: 100
- Retail: 50
- Education: 25
- Gov. and Public: 20
- Financial: 10

Number of Breaches in 2014

Source: Symantec. As of 2015

$1
Cost of a person’s credit-card record on the blackmarket

$2,000
Potential value of a complete medical record on the blackmarket

freedom to focus
Why do you care about HIPAA compliance?

FOR IMMEDIATE RELEASE
January 2, 2013

HHS announces first HIPAA breach settlement involving less than 500 patients

*Hospice of North Idaho settles HIPAA security case for $50,000*

The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services’ (HHS) $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.

The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop

“This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients’ health information.” said OCR Director Leon Rodriguez. “Encryption is an easy method for making lost information unusable, unreadable and undecipherable.”

The Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification Rule requires covered entities to report an Impermissible use or disclosure of protected health information, or a “breach,” of 500 individuals or more to the Secretary of HHS and the media within 60 days after the discovery of the breach. Smaller breaches affecting less than 500 individuals must be reported to the Secretary on an annual basis.

A new educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information*, has been launched by OCR and the HHS Office of the National Coordinator for Health Information Technology (ONC) that offers health care providers and organizations practical tips on ways to protect their patients’ health information when using mobile devices such as laptops, tablets, and smartphones. For more information, visit [www.HealthIT.gov/mobiledevices](http://www.HealthIT.gov/mobiledevices).

The Resolution Agreement can be found on the OCR website at [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf)
Security Risk Assessments and HIPAA Compliance

Jeff Wussow
Business Development Manager
January 20, 2016
Objectives

• What is a Security Risk Assessment and why do I need one?
• Understand the partnership between RevEHR and MetaStar
• What are the required security Policies and Procedures?
What is an SRA?

A gap analysis to determine your organization’s level of compliance with the HIPAA Security rule

- Physical safeguards
- Administrative safeguards
- Technical safeguards

Resource: Department of Health and Human Services
Office of the Secretary
45 CFR Parts 160, 162, and 164
Health Insurance Reform: Security Standards; Final Rule
What is an SRA?

No single method or “best practice” that guarantees compliance

- Review existing infrastructure against legal requirements and industry best practices
- Identify potential threats
- Assess the impact
- Prioritize risks
What is an SRA?

Just having certified EHR technology does not fulfill this security risk analysis requirement.
Who needs a Security Risk Assessment?

- **Everyone** – An SRA is required for compliance with the HIPAA Security Rule for any entity that handles ePHI.

- For those participating in the Meaningful Use Incentive Program – A Security Risk Assessment (SRA) is required for attestations.
MetaStar’s SRA

MetaStar offers a convenient and cost-effective Virtual SRA.

- Risk assessment specialist
- Online tool available 24/7
- Vulnerability scan
- Final report indicating risks and risk priorities
- Remediation plan
- NIST standards
Security Updates & Action Plans

- Write and implement core security policies and procedures
- Correct processes, workflows, policies
- Update software
- Implement training and awareness programs

Resource: CMS Security Risk Analysis Tipsheet
After your SRA

- Ongoing risk mitigation plan
- Policies & procedures
- Best practices
HIPAA Audits

2015 OCR audits focused on
• Device and storage media controls
• Transmission security
• Privacy rule safeguards

2016 OCR audits will focus on
• Encryption
Preparing for Audits

Retain meaningful use documentation for six years post-attestation

- Security Risk Analysis
- Type of SRA completed
- Date(s) SRA completed
- Actions taken to address identified risks

Maintain a list of providers and facilities included in the SRA
Importance of Policies & Procedures

Your SRA references many policies and procedures.

The most frequent reasons practices fail audits were the lack of policies and procedures, or insufficient policies and procedures.
New Service from MetaStar

- Expert guidance on required 13 policies you need for HIPAA security compliance
- An electronic version of the 13 policies customized for your practice or clinic and a binder for your completed, finalized policies
- Peace of mind knowing you’ve helped reduce your risk of failing a HIPAA audit and being subject to substantial penalties
- Designed to be the quickest and easiest process possible for your practice or clinic
MetaStar Policies & Procedures

- Policies & Procedures Specialist
- Online tool available 24/7  A sample questionnaire is available at: https://www.surveygizmo.com/s3/2211190/Demo-Policies-Procedures-Questionnaire
- Physical binder with a USB drive containing 13 policies and procedures
- Wrap up discussion with expert advice and guidance for finalizing the policies & procedures
- Custom policies and procedures review service available
Top 5 SRA Questions from RevolutionEHR Customers

1. Doesn’t RevolutionEHR handle this for me?
2. Do I need to worry about this if I’m not doing MU?
3. Do I need to perform a complete SRA each year?
4. Cost? Do I need to pay someone to perform my SRA?
5. Why should I work with MetaStar vs. someone else?
Contact us

MetaStar, Inc.
2909 Landmark Place
Madison, WI  53713

800-362-2320

www.metastar.com

jwussow@metastar.com