InfoGard Healthcare Services

© 2015 InfoGard Laboratories Inc.

10 Steps To Protect My Covered Entity From Breach

© 2015 InfoGard Laboratories Inc.

Your Presenters

Alan Martin

Account Manger

Marvin Byrd

Security Engineer

© 2015 InfoGard Laboratories Inc.

Test and Certification Laboratory

- Healthcare
- Payment Systems
- Federal Programs

© 2015 InfoGard Laboratories Inc.

Healthcare Services

- **ONC HIT Certification Program** – Accredited Testing Laboratory and Authorized Certification Body for Electronic Health Records (EHR)
- **DEA EPCS Certification Program** – Approved Certifying Organization
- **Security Risk Assessment** (SRA) and Analysis for MU and HIPAA

InfoGard was the first organization approved by the DEA to test and certify applications for Electronic Prescriptions for Controlled Substances (EPCS)

© 2015 InfoGard Laboratories Inc.

HIPAA Security Rule

The HIPAA Security Rule (45 CFR 164.3081) requires that an organization,

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

© 2015 InfoGard Laboratories Inc.

Civil Enforcement

Department of Health & Human Services (HHS)

Office for Civil Rights (OCR)

OCR is authorized to level fines starting from $10,000 based on willful neglect of compliance.

© 2015 InfoGard Laboratories Inc.

HIPAA Facts

Over the past two years:

- 91 percent of healthcare organizations had one data breach
- 39 percent experienced two to five data breaches
- 40 percent had more than five data breaches
- two-thirds of respondents do not offer any protection services for patients whose information has been breached

Source: *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data*

© 2015 InfoGard Laboratories Inc.

HIPAA Facts

A patient's record can be worth as much as $50 on the black market, while a credit card or social security number is valued at only around $1!

$50

= 50X

$1

© 2015 InfoGard Laboratories Inc.

The Ten Steps

© 2015 InfoGard Laboratories Inc.

STEP 1: Security Risk Assessment

Identify the Risks.

Essential to use staff trained in SRAs or an expert.

The HIPAA security rule is a great resource.

Put yourself in the mind of an attacker and attempt to gains access to EPHI.

Consider all reasonable types of attackers and threats.

© 2015 InfoGard Laboratories Inc.

Liability in Detail

Negligence	Minimum	Maximum
in the case of a violation of such provision in which it is established that the person did not know (and by exercising reasonable diligence would not have known) that such person violated such provision	$100/record total of $25,000 cumulative for breach group	$50,000/ record total of $1.5 million cumulative for breach group
in the case of a violation of such provision in which it is established that the violation was due to reasonable cause and not to willful neglect	$1,000/record total of $100,000 cumulative for breach group	$50,000/ record total of $1.5 million cumulative for breach group
in the case of a violation of such provision in which it is established that the violation was due to willful neglect - AND - the violation is corrected	$10,000/record total of $250,000 cumulative for breach group	$50,000/ record total of $1.5 million cumulative for breach group
in the case of a violation of such provision in which it is established that the violation was due to willful neglect - AND - the violation is not corrected	$50,000/ record total of $1.5 million cumulative for breach group	$50,000/ record total of $1.5 million cumulative for breach group

(Source: American Medical Association)

© 2015 InfoGard Laboratories Inc.

STEP 2: Risk Management Plan

Identify the threats and their risk level.

Decide how each threat is going to be addressed.

Assign a time frame on when the controls should be implemented.

Assign the necessary resources.

Assign responsibility to a staff member.

© 2015 InfoGard Laboratories Inc.

STEP 3: Gap Analysis

Evaluate Security Controls to ensure that they are providing the expected protections.

Review password guidelines.

- Verify compliance
- Test effectiveness

Check that new software is configured correctly.

Test contingency plans.

© 2015 InfoGard Laboratories Inc.

STEP 4: Train Staff

Keep your staff trained and aware of security issues.

Making staff aware of security controls can be the easiest was to secure EPHI.

Staff training comes in two categories:

- Ensuring they have the capabilities to perform their job function.
- Ensuring that they are knowledgeable about the policies and procedures currently in place.

© 2015 InfoGard Laboratories Inc.

STEP 5: Network Protection

Vulnerability scanning

- External vulnerability scanning is critical to know that your infrastructure is safe from the external world.
- Internal vulnerability scanning can reveal ways that the infrastructure could be compromised from internal use.

Anti-malware software can address a large percentage of vulnerabilities at a low cost.

- Keep it up to date as new malware is being created every day!

© 2015 InfoGard Laboratories Inc.

STEP 6: Contingency Planning

When a disaster occurs normal operating procedures may quickly become obsolete, especially if human life is at stake.

Keep a set of policies and procedures on how to respond in the event of a disaster is critical for business continuity and ensuring health care information remains safe.

Having an established chain of command and decision making will help organize staff members.

Having current staff exercise the contingency plan will avoid a lot of confusion when time is critical.

© 2015 InfoGard Laboratories Inc.

STEP 7: Monitor Access

Control authorized access to PHI.

Review:

- IT access logs
- Physical access tokens

Set up automatic alerts for suspicious access.

A quick response might make the difference between ending up on the breach list, or just facing a few fines.

Account for all physical tokens to prevent unauthorized access.

© 2015 InfoGard Laboratories Inc.

STEP 8: Automation

Invest in automated systems.

Save payroll costs.

Cameras and auditing tools take out the “human factor”.

Recording for forensics. If there is a breach - this can help the recovery process.

© 2015 InfoGard Laboratories Inc.

Step 9: Business Associates

Require a security risk assessment/risk management plan from every business associate.

This is a great indicator of how serious a third party is about protecting PHI as these are explicitly required by HIPAA.

While the Omnibus rule places much more fiscal liability on subcontractors, the reputation of a covered entity can take many years to repair.

When you end up on the breach list there is a risk of large staff turnover to avoid damage to the individuals reputation.

© 2015 InfoGard Laboratories Inc.

Step 10: Mobile Devices

The HIPAA security rule also applies to mobile devices.

This includes things like transmission security & encryption, auditing, access control etc…

A lost phone containing EPHI would be considered a breach.

Consider having the organization provided cell phones/tablets.

© 2015 InfoGard Laboratories Inc.

Summary

1. Security Risk Assessment
2. Risk Management Plan
3. Gap Analysis
4. Train Staff
5. Network Protection
6. Contingency Planning
7. Monitor Access
8. Use Automation
9. Manage Business Associates
10. Manage Mobile Devices

© 2015 InfoGard Laboratories Inc.

Questions?

Submit questions about this presentation, HIPAA requirements or Security Risk Assessments to sra@infogard.com

InfoGard's technical staff will be answering the questions and posting the answer's on InfoGard's Health IT blog throughout National Health IT Week.

If you are interested in InfoGard's SRA services, contact sales@infogard.com

© 2015 InfoGard Laboratories Inc.