Reinhart Attorneys at Law CLE SERIES

TECHNICALLY CHALLENGED BY CYBERSECURITY RISK MANAGEMENT?

November 15, 2016

Heather Fields, JD, CHC, CCEP
(414) 298-8166
hfields@reinhartlaw.com

Justin P. Webb
(414) 298-8364
jwebb@reinhartlaw.com

Reinhart Boerner Van Deuren s.c.
1000 North Water Street, Suite 1700, Milwaukee, WI 53202
www.reinhartlaw.com

Heather L. Fields is a shareholder in the firm's Health Care Practice and chairs the firm's Hospitals and Health Care Systems group. She is also a member of the firm's Corporate Compliance and White Collar Litigation, Health Care Transactions, Hospice and Palliative Care group and the Tax-Exempt Organizations group. Heather routinely assists clients with a wide variety of regulatory, transactional and compliance-related matters. She has extensive experience advising clients in connection with fraud and abuse issues that arise in the context of various health care provider relationships and transactions.

Justin P. Webb is an attorney in Reinhart's Litigation Practice. Prior to joining the firm, Justin completed a judicial clerkship with the Honorable J. P. Stadtmueller of the U.S. District Court for the Eastern District of Wisconsin.

Reinhart Boerner Van Deuren s.c. Attorneys at Law

Webinar Housekeeping

Viewing the Slides
Today's slide presentation will advance automatically in synch with the live presentation.

Handouts
If you would like a hard copy of the slide presentation, a printable version was e-mailed to you yesterday.

Adjusting Your Volume
Volume can be adjusted using the volume control on your computer or phone.

Asking Questions
Throughout the webinar, type your questions using the "QUESTIONS" section in the webinar panel. We will answer as many questions as possible during our Q & A session at the end of the presentation.

Information
This webinar provides general information about legal issues. It should not be construed as legal advice or a legal opinion. Attendees should seek legal counsel concerning specific factual situations confronting them.

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Data Security—It's Not Just for Plans and Providers Anymore

- It's not Rapidly evolving regulatory landscape—many players (and landmines) at state and federal level
- Industry standards hard to pin down—contractual obligations generally exceed statutory/regulatory duties
- Increasing area of enforcement
- Most significant threat to data may be internal, not external

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Overview

- Types of data that must be protected
- Top Five "Cyber" Best Practices
  - Engage board
  - Assess risk and develop risk management strategy
  - Prepare for breach
  - Manage vendor/customer contracts
  - Train

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What "Data" Must be Protected?

- **PII**: Typically, state laws define personally identifiable information (PII) as an individual's first name or initial with last name, and one or more of the following (unencrypted) data elements:
  - Social Security number
  - Driver's license number or state or military identification card number
  - Financial account, credit card or debit card number in combination with any required security code, access code or password that permits access to an individual's account
- However, some states define PII more broadly to include:
  - Medical information
  - Health insurance information
  - A user name or e-mail address, in combination with a password or security question and answer that permits access to an online or financial account or resource

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

What "Data" Must be Protected? (cont.)

- **PHI**: Protected Health Information (defined under HIPAA)
  - Created by a covered entity
  - Includes demographic information
  - Must be protected by BAAs (*e.g.*, lawyers)
- Examples:
  - Claims data
  - Health plan enrollee data
  - Registration data
- NOT covered entities: worker's compensation claims data, life insurance data

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

PHI/PII Status Is Immutable

- PII and PHI do not lose protection when disclosed to vendor or other related party
- Legal requirements for de-identification not well understood and no clear industry standard
- Understand your place in the data chain
  - Vendor using PII?
  - Business Associate using PHI?
  - User of PHI/PII?

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Top Five Cybersecurity Best Practices to Implement NOW!

- Step 1: Take it to the Top
- Step 2: Assess and Manage Risk (Rinse and Repeat)
- Step 3: Get Ready for a Breach…It's Coming (Soon?)
- Step 4: Contract Responsibly
- Step 5: Get the Message Out

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Step 1: Take it to the Top

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Corporate Governance

- **Does your board review and approve top-level policies on privacy and IT security risks?**
  - 23% - regularly
  - 28% - occasionally
  - 42% - rarely or never
- **Does your board review and approve annual budgets for privacy and IT security programs?**
  - 28% - regularly
  - 10% - occasionally
  - 54% - rarely or never

Carnegie Mellon CyLab 2012 Report

Speak Truth to Power

- **C-level executives take the heat for breaches**
  - A recent Veracode study found that a majority of board members polled blame CEO rather than security team for a data breach
  - Target CEO was fired
- **SEC holds directors responsible**
  - "Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities."

CF Disclosure Guidance: Topic No. 2, Cybersecurity, Oct. 13, 2011

How to Protect the Board/Executives

- Security training
- Security expertise on board and/or consider consulting and retaining outside experts
- Exposure to and education concerning budgets and risks related to data security

Step 2: Assess and Manage Risk (Rinse and Repeat)

Assess and Manage Risk

- Many "frameworks," same goal
- Remember HIPAA compliance does not equal security
- Decide upon a process and stick to it
- Security is a journey not a destination, continuous quality improvement key
- Consider role of attorney client privilege

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

First Principles

- Know your data:
  - What kind(s) do you have?
  - Where is it stored and for how long?
  - Who has access (and who *should* have access)?
  - How is it secured?
- Review, assess policies and practices for data:
  - Collection, storage, use, disclosure, protection, destruction
- Scale down
  - Collect only what you need
  - Keep it only as long as you need it
  - Restrict access

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Next Principles

- Develop a proactive, not reactive information security plan and team—an equal balance of individuals yelling fire and telling everyone to calm down
- Unless you have an underdeveloped program, avoid hyper-focus on operational aspects of InfoSec
- If the technical ability is lacking, avoid hyper-focus on strategic aspects and metrics in larger enterprises,
- Know your attack surface
- **Establish a baseline**
- Enforce record retention policies

Next-Next Principles

- Cybersecurity frameworks
  - NIST/ISO
  - HIPAA Security Rule
  - Attorney General Guidance (*i.e.*, California)
- Lesser Included
  - SANS Top 10
  - OWASP Top 10
  - Open source frameworks and guidance
  - Staying up to date on the landscape
    - Periodic presentations to leadership

Ideal World

- Encryption
- Intrusion detection/prevention
- Mobile device management
- DLP
- Skills-based user education (e.g., PhishMe)
- Social media monitoring
- Two-factor authentication everywhere
- Locked down firewalls
- Internal penetration testing

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Essential Policies and Procedures

- Incident response plan
- Mobile device management
- Updated employee handbook
- Acceptable use policy
- Business continuity policy with InfoSec input
- General information security policy
- User agreements
- **NOTE: This is IN ADDITION TO HIPAA**

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Where the Vulnerabilities Are

- Employees
- Vendors
- Third-party data storage
- Physical environment
  - Firewalls, network infrastructure, Wi-Fi
  - Outward facing interfaces (webpages, portals, etc.)
  - Endpoints (desktops, laptops, printers, cell phones

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Best Practices for Auditing and Testing

- Consider retaining an outside consultant to perform tests of your systems
  - Ethical hacking (penetration testing)
  - Table top exercises
  - Vulnerability scanning
  - Internal/external phishing
  - Spear phishing

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Keep an Eye On

- Data breach notification law updates
  - Some laws updated to include credentials
- Effect of social issues on InfoSec posture
- The changing standard of care
- News from the "underground"

Step 3: Get Ready for a Breach…It's Coming (Soon?)

Get Ready for a Breach…It's Coming (Soon?)

- Do you have an incident response plan?
- Do employees know how/when to report data incidents?
- Consider interrelationship between "HIPAA Breach Policy" and IT incident response procedures
- Insurance

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

How Does a Data Breach Occur?

1. Malicious Internet attacker/APT
2. User error
3. Loss/theft of device
4. Disgruntled employee
5. Third-party mistake
6. Other

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Cost of a Data Breach

- Data security breaches are a key risk area for businesses. A business that suffers a data breach incident or reportable event may incur significant expenses, including costs relating to:
  - Investigating and containing the breach
  - Notifying affected individuals if the breach affects individuals' PII
  - Government fines and private lawsuits
  - Reputational damage and lost business

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Best Practices for Cyber Liability Insurance

- Review policy and understand exactly what is covered
  - Policies tend to define breach incident differently
- Review the policy with the information security team
- Does it cover external breaches only? Internal?
- What are the exceptions?
- Realize that the norms are being established

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Step 4: Contract Responsibly

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Do You Know What Your Contracts Require?

- Attorneys:
  - With increasing frequency, clients are seeking security reps and warranties in engagement agreements
  - Many firms have not instituted BAA process to ensure obligations align with contract party position
- Clients:
  - Vendor due diligence is a must
  - Consider risk-based approach to managing vendor security agreements/contract standards

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Best Practices Continued: Vendor Contracts

- Review contracts with vendors that collect, provide, access, use, disclose PHI/PII
  - Do contracts have indemnification provisions?
  - Does vendor have resources to indemnify?
  - Do your vendors have cyber liability insurance coverage? Do you have coverage?
  - Data breach clause essential (REQUIRED BY HIPAA):
    - ✓ Notification process and timing
    - ✓ Cooperation during investigation
    - ✓ Who notifies affected parties?
    - ✓ Who pays for notice?
    - ✓ Clear delineation of responsibility

Step 5: Get the Message Out

Strengthen the Weakest Link

- Education and training is key
  - Employee education upon hire, annually thereafter, notice of updates to procedures
  - Document
- Well wunderstoon and publicized reporting procedures essential
- PII/PHI avoidance requires advance communication with clients
  - Remember minimum necessary

Reinhart
Boerner Van Deuren s.c. Attorneys at Law

Questions?

THANK YOU!

Reinhart
Boerner Van Deuren s.c. Attorneys at Law