34TH ANNUAL ISCEBS
Employee Benefits
Symposium

Data Breach and Cybersecurity: What Happens If You or Your Vendor Is Hacked

Linda Vincent, R.N., P.I., CITRMS
Vincent & Associates
Founder
The Identity Advocate
San Pedro, California

PARTNERS IN EDUCATIONAL EXCELLENCE
International Society of Certified Employee Benefit Specialists
International Foundation of Employee Benefit Plans

Agenda

- What is Medical Identity Theft?
- What is at risk?
- How does cyber hacking affect your participants?
- Should you consider cyber liability insurance
- Ensuring security with external partners
- Critical steps in face of security incident

What Is Medical Identity Theft?

Medical Identity Theft occurs when someone uses your personal information to:

- Fraudulently procure medical services
- Improperly acquire prescription drugs
- Submit fake billings to Medicare or private insurers
- Obtain expensive medical equipment

Impact of Medical Identity Theft

- Death
- Medical records in shambles
- Physical harm
- Credit issues
- Employment issues
- On the hook for thousands of dollars
- Long term recovery and dispute resolution

Stealing Your Medical Identity

How?

- Cyber hackers/thieves via the web & mobile devices
- Malware on facility computers
- Misdirected emails, improper disposal of paper records

Who?

- Dishonest patients
- Dishonest providers (individuals or institutions)
- Professional criminals/bogus providers

Where?

- Doctors and hospitals
- Insurance companies
- Fund offices

2014 IDTRC Breach Survey*

- Of 80 healthcare organizations > 40 incidents
- 783 breaches exposed 675 MILLION records
- Breaches average 416 days to detect
- Breaches often reported by 3rd party
- 94% of providers have HC information breeches
- Medical ID Theft occurs in 24% of breaches!

* Identity Theft Resources Center 2014 Data Breach by Category Report

Healthcare Data Breaches Ex.

- **Tricare:** 4,901,432—Loss of backup tapes
- **Health Net:** 1,9000,000—Unknown reason
- **Anthem:** 80,000,000—Cyber hacking
- **Taft-Hartley/Public Health Funds:** Lost laptops, CDs, SSNs externally visible, paper records in dumpster

* Net Diligence 2014 Survey

Cost of Cyber Crime Report*

- **$6 million:** The median annualized cost of an attack
- **$60 million:** Total annualized cost of companies surveyed

  Cost of Crime: influenced by frequency of attack and type
- **1.7:** The number of *successful* attacks per week

  Attacks from worms; malware; botnets; web based; phishing; malicious code; denial of service; stolen devices; malicious insiders
- **26%:** The increase in cyber attacks in one year

* 2014 Global Report on the Cost of Cyber Crime (257 cos.)

How Cyber Hacking Can Affect Fund or Participants

- Regulatory compliance
  - Remediation is expensive and time consuming
  - Aggressive laws and Attorneys General
  - Non-Compliance can lead to fines (HIPAA, State)
- Reputational harm: Loss of confidence
- Financial loss plan sponsor or employees
- Litigation from impacted parties

State Laws on Data Breaches

****50 States; 47 Different Sets of Rules****

- Identity theft laws
- Consumer report laws
- Security breach notifications
- Laws protecting SSNs
- Personal information laws
- Possible private rights of action

- (Alabama, New Mexico, South Dakota)

Breach Obligations

- Notification to breached party?
- Notification to all, breached or not?
- Notification to media?
- Offer credit monitoring/ID theft protection?
- Offer recovery?
- Is the breach really over?
- Whose obligation is it?

Vendor Breach Considerations

- Begin with review of Business Associate Agreements
- Who owns or is responsible for the data?
- Sit-back or be active?
- Respond: Together? Separately? Not at all?
- 20% of breaches triggered by 3rd party
- Look to contractual relationships for assumption of responsibility.
- Whose insurance responds and when?

Do Participants Have Protections?

Participants and beneficiaries are relying on the benefit plan officials' legal obligations to protect their information.

- ERISA
- Trust law
- Consumer protection laws
- Contract language with vendors/business associates
- Other legal recourse?

Member Obligations Avoid Data Losses

- Always check EOBs, billing statements, credit reports
- Request/review/annual ‘benefits paid’ from insurer
- Keep your own copies of all your health records
- Review accuracy of medical records
- Eliminate SSN and total DOBs from records
- Freeze your credit with each agency

Ways to Avoid Data Losses *cont.*

- Never share your health insurance card
- Shred all medical documents
- Never partake of **“free”** medical care
- Don’t discard prescription bottles with your (or your pet’s) information label still affixed
- Report and replace lost/stolen insurance cards

Protection for Funds

- Policies on bringing devices to work (BYOD)
- Policies on taking work home/device home
- Policies on Social Media, internet access, cloud usage
- Background checks on all employees
- 256-bit encryption for file transfer or claims payments
- Two-factor authorization

Risk Assessment

- Required by HIPAA/HITECH for H&W benefit plans
- Identity and evaluate plan's data protection and destruction practices
- Document the security gaps
- Proposes possible solutions
- Not a one-time event

Eliminate or Minimize the Risk

- Monitor and test security systems often
- Minimize collection of personal data, destroy unneeded
- Invest in data security software
- Create position of Chief Information Security Officer
- Encrypt! Encrypt! Encrypt!
  (Generally a Safe Harbor)

Critical Steps in Face of Security Incident

- Essential in order to effectively respond to a security breach
- Periodically tested under various breach scenarios
- Incident Response Plan typically include:
  - IRP Team (Administrative Management, IT Professionals, and Fund Counsel, etc.)
  - Clear guidelines categorizing threat levels
  - Documentation guidelines
  - Notification process including contact information

Cyber Liability Insurance

- Insurance is often a cost effective solution.
- Premiums for this particular coverage are now very affordable for most plans.
- A employer's other insurance policies do not provide the needed protection since *these policies were not designed for these exposures*.

Cyber Liability Insurance

- Used to protect plan assets
- Helps meet legal obligations
- Provides various professionals to assist in handling a data breach event
- Offers participants certain protections

Comprehensive Coverage!

- Provides partial to full risk transfer that risk assessments and IRPs do not eliminate
- Provides experienced professionals
- Provides data-packed web sites to help create a robust internal control environment
- Provides first-party cost coverage not available in other policies
- Protects against third-party liability

Current State of the Market

- Evolving coverage; broader and cheaper
- Many carriers; many approaches
- Different risk appetites; size/complexity
- Modular; buy only the coverage you need

Covered First Party Costs

- Notification
- Public relations/crisis management
- Call center operations
- Credit monitoring
- Forensics
- Other potential expenses

Third-Party Liability Coverage

Triggered by a claim:

- Against the plan
- Alleging a “loss”
- Based on a “wrongful act”
- Provides defense, settlements, judgments

Conclusion

- Health plans are rich in resources
- Breaches/Hackers are everywhere
- Review Business Associates agreements
- Medical ID Theft can be expensive to remediate
- Legal compliance is complex

What Can Plans Do?

- Develop an Incident Response Plan (IRP)
  - Identify the risk issues—Preparation
  - Mitigate the risk—Detection and Analysis
  - Preplan and practice a response
- Risk transfer
  - Cyber liability insurance

Key Takeaways

Plan to Act NOW!

- Evaluate your risk
- Review your Business Associate Agreements
- Protect and control your data
- Plan a response for when it gets out
- Consider cyber liability insurance
- Understand coverage: Loss of data vs Theft of data

QUESTIONS

- Thoughts
- Concerns

Thank you!

Other thoughts and considerations

Federal Obligations

Protecting PII

- Fair Credit Reporting Act
- Fair and Accurate Credit Transactions Act
- Gramm-Leach-Bliley Act
- Federal Trade Commission

Protecting PHI

- Health Information Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)

What About ERISA?

- Does not directly address how plans should protect PII/PHI.
- Will ERISA preemption apply?

Reasonable Conclusion:

Plans have to comply with many of these state disclosure and notification laws because there are no overall federal guidelines and ERISA does not directly apply.

Still a Fiduciary Risk?

Failure to protect PII/PHI may be a significant fiduciary risk!

- **Be concerned:** Fiduciary responsibility likely applies!
- **Be diligent:** It is often the *process* that determines your liability rather than the outcome of your efforts.