EPSTEIN
BECKER
GREEN

HIPAA, HITECH and Privacy

How to Manage Privacy and Security Risks and Considerations

Presented by

Patricia Wagner

Member of the Firm

pwagner@ebglaw.com

202-861-4182

Privacy and Security Considerations

- Privacy
  - Who has access to the data?
  - What can be done with the data?
  - How is data protected from misuse?

- Security
  - How is data secured?
  - How is security monitored?
    - Audits
    - Logs
    - Other?

Enforcement

- Department of Health & Human Services, Office for Civil Rights
- State AGs
- Federal Trade Commission
- Private Plaintiffs

Privacy in State of Union Address

- Reported that the State of the Union Address will include new initiatives related to privacy
  - Setting a national data breach reporting standard
  - Student Digital Privacy Act (restrict sale of student data)
  - Consumer Privacy Bill of Rights (reportedly would ensure more control over personal data for individuals, more closely in line with the rules in place in the European Union).

The HIPAA Privacy Rule

- The HIPAA Privacy Rule (the "Privacy Rule") is a set of regulations that requires certain entities to maintain and protect the privacy and security of individually identifiable health information (also known as "protected health information" or "PHI").

Mantra of HIPAA Privacy Rule

- The HIPAA Privacy Standards establish a fundamental presumption that all "Protected Health Information" is confidential, and can only be disclosed with appropriate authorization from the individual
- Exceptions to this presumption are limited

HIPAA Security Rule

- Requires protection of electronic PHI
  - Physical Safeguards
  - Administrative Safeguards
  - Technical Safeguards

HITECH

- Increased penalties for violation of the Privacy and Security Rules
- Directly obligates business associates to certain requirements of the Privacy and Security Rules
- Requires notification in the event of a breach of PHI

What is PHI?

- PHI is information:
  - in any form of medium, oral or recorded (not just electronic)
  - that relates to the individual's health, healthcare, treatment, or payment
  - that identifies the individual in any way
- That means PHI includes:
  - Name, address, birth date, phone and fax numbers, email address, social security numbers, and other unique identifiers
  - Type of doctor being visited (when added to something that could identify the patient)
  - Prescription information, other claims submission data

Examples of PHI for Group Health Plans

- Group Health Plans may have PHI in:
  - Complaints from beneficiaries about whether service is being paid
  - Claim submissions
  - Appeals for denied services
  - Beneficiary support services
  - EAP documentation
  - Flexible Spending plan documentation
  - On-site medical clinics? (not always part of plan but may have special considerations)

Vendors May Have Access to PHI

- Vendors
  - Third party administrator
  - IT service vendors
  - Storage facilities
  - Cloud vendors
  - On-site medical clinics

Privacy Risks

- The “rogue employee”
  - Someone accesses and using information in a way not permitted under the Privacy Rule, or other laws.
- A Vendor’s rogue employee
- A Vendor’s use of the data
  - what contractual rights did they reserve?

Rogue Employee

- Walgreen Case (in Indiana)
  - Pharmacist viewed prescription records of a customer
  - Customer's ex-boyfriend tells customer he has a print out of her records
  - Two years later customer finds out the ex-boyfriend is now married to Walgreen pharmacist
  - Pharmacist maintains she looked at customer's record but never shared it
  - Customer files litigation
  - Trial ensues and jury delivers verdict $1.4 million for plaintiff

Rogue employee

- Court held, and appellate court upheld
  - Employer responsible for acts of employee when conduct is within scope of employment
    - Within scope -- “incidental to job duties or originated in activities closely associated with job
  - As a result Walgreen and individual defendants are jointly liable for $1.4 million

Privacy Gaining More Interest

- Recent Letter from Senator Al Franken related to employees use of information provided to organization
  - Letter request asks for information related to
    - Steps taken to limit access to data by employees
    - Training provided to employees
    - Monitoring processes
    - Disciplinary policies

Other Employee Situations

- The helper (shares information to “help”)
- The deflector (uses privacy to deflect from the other issue)
- The criminal (steals information to sell)
- The case builder (takes information to “bolster” claims)

Managing Employee Risk?

- Training
- Auditing
- Disciplinary actions
- Top down focus on privacy and security
- Clear policies

Privacy Risks

- The “rogue employee”
  - Someone accesses and using information in a way not permitted under the Privacy Rule, or other laws.
- A Vendor’s rogue employee
- A Vendor’s use of the data
  - what contractual rights did they reserve?

Managing Vendor Risk

- Dealing with reputable vendors

- Strong contract language that
  - Protects data rights (may even want to protect data rights of de-identified data)
  - Limits use of data by vendor

Security Risks

- Breach of information
- Breach can occur through
  - Hacking
  - Lost device
  - Errant email
  - Lost mail or package

Sample of Security Breach Affecting Employees

- Sony Breach - Class Action Suit already filed
  - Plaintiffs (former employees) allege that the following information was affected by the breach:
    - A Microsoft Excel document that contains the name, location, employee ID, network username, base salary and date of birth for more than 6,800 people;
    - A status report from April 2014 listing the names, dates of birth, Social Security numbers and health savings account data on more than 700 Sony employees; and
    - A file that appears to be the product of an internal audit from PriceWaterhouseCoopers, made up of screen shots of dozens of employees' federal tax records and other compensation data.

Managing Security Risks

- Strong IT and Security Controls
- Audits
- Scans
- Risk Assessments
- “Dummy” calls

Managing Vendor Risk?

- Strong contracts
  - Responsibility for breaches
  - What happens to data when contract is terminated
- Diligence on vendors
  - How do you safeguard employee information?
  - Have you had any reportable breaches?
  - Do you have an incident response policy?
  - Do you store information or do you use a vendor to do so?
- How do you assess the responses?

Cloud Vendor Special Issues

- Limited negotiation power ("we don't negotiate our agreements")
- May be reluctant to impart details related to security posture (which may be a good sign)
- May charge "a la carte" fees for additional security measures (e.g., pay for meeting obligations of BA agreement)

Business Associate Agreements

- Vendors that use, disclose, or maintain PHI should have a business associate agreement with the plan
- Business Associate Agreement should have provisions required by regulation
- Other provisions
  - De-identification (some vendors include data rights provisions in de-identification provisions)
  - Data aggregation (some vendors craft broad aggregation rights into this provision)
  - Protection in the event of a security breach (indemnification, insurance, other language)
  - Disclaimer of agency

Compliance Tips

- Training
- Monitoring
- Have a Fulsome Complaint Process
- Don’t ignore issues (mitigate)
- Get the full story

Other Areas of Focus for Privacy/Security

- Mobile Devices
  - Phones, Tablets, Laptops
    - Screen locks
    - Encryption
    - Selected Models
    - Limit Storage
    - Limit activities?
- Social Media (Twitter, Facebook, etc. etc)
  - Strong policy, but aware of laws

HIPAA Civil Penalties

Violation Category	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	$1,000–50,000	$1,500,000
(C)(i) Willful Neglect-Corrected	$10,000–50,000	$1,500,000
(C)(ii) Willful Neglect-Not Corrected	$50,000 1,500,000	$1,500,000

Criminal Penalties Can Also Apply

Questions?