Cybersecurity Laws, Breach Notification Laws, and Privacy Laws & Your Legal Practice

Maraleen D. Shields, Esq.

- Shareholder of Fitzpatrick, Lentz & Bubba's Healthcare and Litigation Groups
- Represent healthcare providers on a variety of matters, including HIPAA/HITECH, medical staff, licensure disputes, patient safety
- Member of American Health Layers Association

AGENDA

Potential Risk Areas for Attorneys/Law Firms

Legal and Professional Obligations

Tips & Takeaways

CURRENT LANDSCAPE

Information Handled By Attorneys/Firms

Classification of Information

1) Public Information
2) Confidential Information
3) Highly Confidential Information
    - Information subject to additional legal protections or handling requirements
        - Personal Information
        - Personal Health Information (PHI)

Sources of Highly Confidential Information

Clients

Opposing Party

Employees

Hackers
Client Demands
Spammers
Employees
Phishers
Changing Legal Framework
Ransomware
THREATS ARE EVERYWHERE

What Do I Have to Lose?

- Lost Data
- Lost Productivity
- Data Breach Expenses
- Civil Lawsuit Expenses
- License
- Civil Penalties
- Criminal Penalties
- Reputational Loss

LEGAL & PROFESSIONAL OBLIGATIONS

Legal & Professional Obligations

Breach of Personal Information Notification Act

Health Insurance Portability and Accountability Act (HIPAA)

Pennsylvania Rules of Professional Conduct

Dittman v. UPMC

Breach of Personal Information Notification Act

73 P.S. § 2301 et al.

Breach Notification Requirement

The Duty

An entity that maintains, stores or manages computerized data that included personal information shall provide notice of any breach of the security …

73 P.S. § 2303

What is an Entity?

A State agency, a political subdivision of the Commonwealth or **an individual or a business doing business in this Commonwealth**.

73 P.S. § 2303

Breach Notification Requirement

The Duty

An entity that maintains, stores or manages computerized data that included personal information shall provide notice of any breach of the security …

73 P.S. § 2303

What is Personal Information?

Personal Information – An individual's first name or first initial and last name and the following encrypted or redacted information:

- Social security number
- Driver's license number or a State identification number
- Financial account number, credit or debit card number, etc.

73 P.S. § 2302

Breach Notification Requirement

The Duty

An entity that maintains, stores or manages computerized data that included personal information shall provide notice of any breach of the security …

73 P.S. § 2303

Breach of Personal Information Notification Act

Breach of Data Security

The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.

73 P.S. § 2302

Encryption Safe Harbor

An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, or access to encryption key is obtained.

73 P.S. § 2303(b)

Breach Notification Requirement

The Duty

An entity that maintains, stores or manages computerized data that included personal information shall provide notice of any breach of the security …

73 P.S. § 2303

Breach of Personal Information Notification Act

When Does Notice Need to Be Given?

…in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made **without unreasonable delay**.

73 P.S. § 2303(a)

Notice may be delayed for law enforcement purposes. 73 P.S. § 2304

Notice to Consumer Reporting Agencies

If more than 1,000 are affected, entity shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis

73 P.S. § 2305

What is Notice?

May be provided by any of the following methods of notification:

1) Written notice

2) Telephone notice

3) E-mail notice

73 P.S. § 2302

Breach of Personal Information Notification Act

Substitute notice permissible if:

a) Cost of providing notice would exceed $100,000;
b) Affected class of individuals to receive notice exceeds 175,000; and
c) Entity lacks sufficient contact information.

Substitute notice consists of <u>all</u> of the following:

a) E-mail notice (no requirement of prior business relationship);
b) Conspicuous posting of notice on entity's website; and
c) Notification to major statewide media.

73 P.S. § 2302

Vendors

Vendor must report to entity.

Entity retains responsibility under the Act to provide notice.

73 P.S. § 2303

Breach Notification Requirements

Violation of Unfair Trade Practice and Consumer Protection Law

Enforcement by Pennsylvania Attorney General

No Private Right of Action

Health Insurance Portability and Accountability Act (HIPAA)

45 C.F.R. Parts 160, 162 and 164

HIPAA

Designed to provide security and privacy for certain health information of individuals called protected health information

HITECH

Extended HIPAA regulations to business associates

Expanded breach notification requirements

Who is Governed by HIPAA?

HIPAA Applies

Covered Entities (CE)

- Health Plans
- Health Care Providers
- Health Care Clearinghouses

Business Associates (BA)

Provide a service in which PHI is disclosed

HIPAA Does Not Apply

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- State agencies (such as child protective services)
- Most law enforcement agencies
- Many municipal offices

Business Associate Agreement

An agreement between a CE and a BA
(or between a BA and its subcontractor)
that is *required* to be in *writing*.

What is Protected by HIPAA/HITECH?

Protected Health Information (PHI)

- Individually Identifiable Health Information

PHI EXAMPLES

Medical Record Contents

Conversations with Health Care Providers

Information in a Health Insurer's Computer System

Billing Information

Insurance Cards

HIPAA/HITECH RULES

- Privacy Rule
- Security Rule
- Breach Notification Rule

- Required, permitted, and prohibited uses and disclosures
- Ensure confidentiality, integrity, and availability of all PHI that the entity creates, received, maintains or transmits
- Notification in the event of breach of unsecured PHI

REQUIRED AND PERMITTED USES AND DISCLOSURES

REQUIRED

To individuals requesting access or accounting of disclosures of their PHI

To HHS when it is undertaking a compliance investigation or review, or enforcement action

PERMITTED

Treatment, payment, and health care operations

Opportunity to agree or object

Incident to an otherwise permitted use and disclosure

Public interest and benefit

Limited data set for purposes of research, etc.

Authorized Uses and Disclosures

All other uses and disclosures of PHI require written authorization of the individual

- Plain language
- Specific information to be used/disclosed
- Person(s) receiving information
- Expiration (or statement of no expiration)
- Right to revoke

HOW IS PHI PROTECTED?

1. Safeguards (physical and technological) to PHI
2. Reasonably limit use and disclosure to minimum necessary
3. Processes to limit who may view and access PHI
4. Duties extend to BAs

KEY BAA CONSIDERATIONS

Terms/ Privacy Standard

Consistent with HIPAA

BA Obligations

- PHI Protection
- Breach
- Accounting

Permitted Uses and Disclosures

CE Obligations

- Changes to Permitted Uses and Disclosures
- Notices of Privacy Practices

Terms/Privacy Standard

- Upon BA Breach
- Record Destruction or Return

Costs

Choices of Venue, Law

WHEN A BREACH OCCURS

All affected individuals must be notified if CE or BA knows, or reasonably believes, security of PHI has been breached

Notification within a reasonable time, not longer than 60 days

NOTIFICATION CONTENT

INDIVIDUALS

- Description of breach
- Date of breach
- Date of discovery of breach
- Description of information put at risk
- Mitigation efforts and steps individuals may want to take
- Contact information, including toll free number

HHS

- If 500 or more individuals, notice at same time as individuals
- If less than 500 individuals, notice within 60 days of end of calendar year

MEDIA NOTIFICATION

If breach involves 500 or more individuals, CE or BA must send press release within 60 days

ENCRYPTION SAFE HARBOR

COMPLIANCE AND INVESTIGATION

- All complaints must be investigated
- Options for handling include:
  - HHS determination that no action necessary
  - HHS attempt to resolve the matter informally
  - HHS starting a formal processing giving CE or BA notice and time to provide mitigating factors
  - HHS imposing civil monetary penalty
  - Resolution agreement
- No private right of action

HIPAA CIVIL PENALTIES

Type of Violation	Min-Max Amount per Violation
Without Knowledge	$100-50,000
Reasonable Cause	$1,000-50,000
Willful Neglect (corrected)	$10,000-50,000
Willful Neglect (not corrected)	$50,000-no cap

HIPAA CRIMINAL PENALTIES

One who **knowingly** obtains or discloses PHI faces fine of $50,000 and up to one-year imprisonment.

False pretenses?
$100,000 fine and 5 years imprisonment

Intent to sell, transfer or use PHI?
$250,000 fine and 10 years imprisonment

Pennsylvania Rules of Professional conduct

LICENSURE EXPOSURE

Duty of Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. Pa.R.P.C. 1.1

Duty of Competence

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Pa.R.P.C. Rule 1.1 Comment 8

Duty of Confidentiality

Pa.R.C.P. Rule 1.6(a)

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Rule 1.6
Confidentiality of Information

Pa.R.C.P. Rule 1.6(d)

A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except disclosures that are impliedly authorized in order to carry out the representation….

Rule 1.6
Confidentiality of Information

Pa.R.C.P. Rule 1.6(e)

The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Applies to your employees too.

Pa.R.P.C. 5.3

Dittman v. UPMC

196 A.3d 1036 (Pa. 2018)

Dittman v. UPMC

2014 data breach of UPMC network

62,000 employees impacted

Social Security numbers, birthdates, confidential tax information, addresses, salaries, bank account information

Alleged that information was used to file fraudulent tax returns

Fall Out: *Dittman v. UPMC*

- Where an employer opts to collect an employee's personal information, the employer has a duty of reasonable care to secure personal information "against unreasonable risk of harm arising out of the employer's data collection practices."
- Personal and financial information not strictly defined, but broader than PA Breach Notification Act
- Not limited to employment context

DITTMAN v. UPMC

NEW DUTY

Not a New Affirmative Duty

Existing Duty to a Novel Factual Scenario

EVISCERATION OF ECONOMIC LOSS DOCTRINE

Source of duty independent from contract

WHY DOES THIS MATTER?

WHY THIS MATTERS

1. Individuals Demand It
2. Law Requires It
3. Licensure May Depend Upon It
4. Costs Can Be Devastating

TAKE AWAY FOR ALL LAWYERS AND LAW FIRMS

Critical Self Assessment

- Assessment
- Robust (and enforced) policies and practices
  - Training
  - How material will be handled
  - Response in the event of breach
- Insurance (cybersecurity)

Commonsense Protections

- Physical Security
- Shredding
- Common Areas
- Minimum Necessary
- Public Wi-Fi
- Credit Card
- Encryption
- Secure File Transfer

Maraleen D. Shields, Esq.

FITZPATRICK LENTZ & BUBBA, P.C.
645 West Hamilton Street, Suite 800
Allentown, PA 18101

PHONE
(610) 797-9000 ext. 376

EMAIL
mshields@flblaw.com

THANK YOU