

Seton Hall Presentation

Overview of Data Protection for Life Science Organizations

March 23, 2016



* Any advice or analysis given by PwC does not constitute legal advice or opinion.

Session Objectives

By the end of this session, you will:

- Understand the privacy laws in the US and around the world at a high-level including cultural requirements and common requirements
- Understand HIPAA, HITECH and the Omnibus Final Rules
- Understand the General Data Protection Regulation (GDPR)
- Understand various breach notification laws and requirements
- Understand various initiatives and techniques that can enhance the robustness of privacy/security program in Life Science Organizations
- Apply your understanding of the laws in a real-world scenario

What is Privacy

- Privacy is the **right of an individual** to limit the collection, use and dissemination of personal information about them
 - The criteria that determines what is considered "private" differs among cultures and regulatory landscapes. However, the **unifying theme** across the different criteria **is a need to protect information that is valuable to the individual**
 - A patchwork of privacy laws and regulations have been established to help ensure that personal information remains private
- Privacy in the **context of a corporation** refers to the organization's responsibility for using the data it has obtained about any individual solely for the purposes that the individual
 - as a data subject, has agreed to, or
 - as a client, would reasonably expect that the organization use to the individual's benefit
- Organizations have **legal** and **ethical** requirements to implement safeguards that will protect the private information they collect
- At its heart, privacy is about ensuring the **expectations of data subjects are met and their data is not misused**

Definitions to Know

- **Personally Identifiable Information (“PII”)**

Any piece of information that potentially can be used to uniquely identify, contact, or locate an individual

Personal information includes Social Security Numbers, Driver's license numbers, bank account, credit card and debit card numbers, health information, health insurance ID numbers and other data elements

- **Sensitive Personal Information (SPI)**

Subset of Personal Information that warrants additional protection. Includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, and data relating to offenses and/or criminal convictions

- **Protected Health Information (PHI)**

Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history for example it also includes a health coverage indicator

Definitions to Know

- **Data Privacy**

Data privacy outlines the measures that enable individuals to exercise control over their personal data

The relationship between the collection and dissemination of personally identifiable information, the individual's expectation of protection against unauthorized access, and the associated technical, legal, and regulatory issues surrounding them

- **Data Security**

Data security is the overarching architecture for protecting all valuable assets

- **Data Protection**

Data protection is the mechanisms with which customers control their personal data. Companies are responsible for making these mechanisms available to their customers, partners, and employees, as well as complying with limitations and conditions on the collection and processing of data about a specific individual

- **Security by Design/Privacy by Design**

Security and Privacy by design is an approach to development that builds in security and privacy protection from the start rather than as an afterthought

Why is Privacy Important?

- Data/Information is a **corporate asset**, like any other but the rights that individuals have over their data/information is protected
- Corporate Data/Information is at **a higher risk** of theft or misuse than ever before¹
 - Organizations have obligations to **protect data**;
 - Laws, regulations, guidelines
 - Contracts with vendors / third parties
- Organizations are therefore subject to commercial risks (loss of competitive advantage, financial, and customer loyalty) as well as potential regulatory implications (lawsuits, investigations, and penalties) in the event of a breach

¹The number of incidents detected in the past 12 months increased by 38%
Source: PwC: Global Information Security Survey 2015

The Global Picture: Data Protection Laws Around the World

- **Europe, Middle East, and Africa**

- The EU's General Data Protection Regulation drives privacy legislation in the EU countries; Companies will have to be compliant by 2018
- Israel recognized for having strong data protection law
- Russia establishing law related to data localization
- Africa with little data protection laws in place

- **North America**

- Canada has federal & provincial laws
- US has multiple state laws & some federal laws
- Mexico has 1 federal data protection law

- **Asia, Australia and New Zealand**

- Increasingly more privacy aware and are enacting new or amending existing data protection laws (e.g., Singapore, Hong Kong, Japan, South Korea, Malaysia)
- Strong data protection laws in place

- **Latin America**

- Several countries have enacted or implemented data protection laws (e.g., Argentina, Colombia, Costa Rica, Perú and Uruguay)

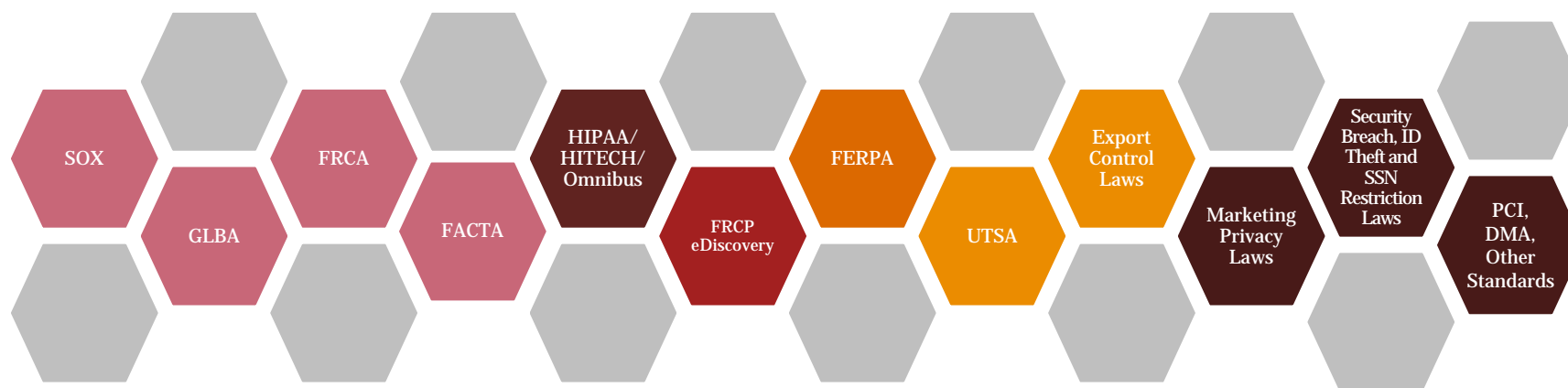


Varying Approaches to Privacy: A World of Difference

Legislative Approach	Sectoral Approach	Omnibus Approach
Types of PI Covered	<ul style="list-style-type: none"> • Financial - GLBA / FCRA / FACTA • Health Care - HIPAA • Children - COPPA • Privacy Marketing Laws • Security Breach & Disclosure 	<ul style="list-style-type: none"> • All Types of Data: EU Data Protection Directive and Other Global Laws
Scope	<ul style="list-style-type: none"> • Primarily Consumers 	<ul style="list-style-type: none"> • Consumers & B-to-B
Enforcement Body	<ul style="list-style-type: none"> • FTC • State Attorneys General • FCC, Industry Trade Groups • Private and Class Actions 	<ul style="list-style-type: none"> • Data Protection Authorities • Labor Works Councils/Union Bodies • Private Rights of Actions
Registration & Data Transfers	<ul style="list-style-type: none"> • No restrictions on transfers across country borders • No filing requirements 	<ul style="list-style-type: none"> • Transfer out of EEA only with “Adequate Protections” • Database & transfer filings

What doesn't vary? Most privacy requirements have, at their cores, the Fair Information Practice Principles (FIPPs).

Key US Federal Laws and Standards



Types US Federal Laws and Standards

Financial
Reporting & Data

Health Data

Archived Data

Student Records

IP/Trade Secrets

All Personal
Information

In addition to the Federal laws listed above, many states have their own laws and regulations regarding security and handling of Personal Information.

Key privacy considerations

US Federal Regulations

FTC Health Breach Notification Rule

- Requires notice after unauthorized acquisition of unsecured PHI

FTC Section 5: Unfair and Deceptive Practices Act

- Broadly prohibits “unfair or deceptive acts or practices in or affecting commerce,” including misleading patients about data use

HIPAA

- Allows for the de-identification of data to minimize regulatory exposure
- Minimum Necessary Rule

State Regulations

California Specific

- The Confidentiality of Medical Information Act (CMIA)
- The Security Breach Notification Law

Majority of States

- Data breach notification requirements are only triggered if the information accessed was unencrypted
- Require a “risk of harm analysis” in determining whether notification is required

May Require Security Safeguards

- MA: Standards For The Protection of Personal Information of Residents of the Commonwealth
- NV: Security of Personal Information
- TX: Medical Records Privacy Act

International Regulations

EU Directive being replaced by General Data Protection Regulation

- Establishing new requirements going beyond EU Directive’s requirements
- Cross border dataflow compliance, accountability, right to be forgotten

Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

- Requires consent by individuals for collection & use of personal information

South America & Asia: Scattered

- Mexico: The Federal Law on the Protection of Personal Data held by Private Parties
- Hong Kong: The Personal Data (Privacy) Ordinance (Cap. 486)
- Argentina: Personal Data Protection Law Number 25,326

Framework Options

NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

- Comprehensive security and privacy controls to be applied within a risk management framework

ISO 27000 Series

- International standard for establishing, implementing, maintaining & improving an info security management system

Privacy from a Consumer's Perspective

- Assert and Protect individuals' rights of privacy.
- Assure the Confidentiality, Integrity and Availability of personally identifiable information by requiring the implementation of certain control measures as safeguards.
- Ensure that individuals are notified of breaches to their personal data including Protected Health Information.
- Ensure that individuals have the right to erasure of their personal data
- Confirm individuals have have the ability to give and withdraw consent that has been explicitly stated

"I can control who uses my personal information."

"Standards/Notice make me feel comfortable that you are protecting my personal information."

"I'll know if something goes wrong within 72 hours and can expect you to be held accountable for inappropriate action."

"I can request to delete my personal data at anytime so that third persons can no longer have my information"

"I'll know exactly what I am consenting to on the behalf of my my child regarding the processing of his personal data and I'll have the ability to withdraw consent at anytime"

Discussion on HIPAA

Overview of HIPAA

What is HIPAA?

- HIPAA stands for **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct. A federal law enacted in 1996 to establish standards for the privacy and security of Protected Health Information (PHI)
- There are 3 sections to manage: HIPAA Security rule, HIPAA Privacy Rule and HITECH breach notification

What Type of Information Falls Under HIPAA?

- Protected Health Information: (e.g., Patient's name, SSN, patient's birth date, patient's account number, medical records, email addresses).
- Essentially any identifiable information that is used in connection with healthcare treatment, payment or operations.

What Type of Information Falls Outside of HIPAA?

- “De-Identified” Information
 - PHI is presumed ‘de-identified’ if it contains no identifiers of an individual, relatives, employers or household members
 - In the US, requires the removal of 18 data identifiers (known as the Safe Harbor method) or statistical analysis that data can't be re-identified (known as the Expert Determination method)
 - EU and other countries will have various requirements for how to de-identify data

To whom does HIPAA apply?

Covered Entities

- Individuals or Organizations that directly handle PHI
- **Health Care Providers** who transmit any health information in electronic form
 - E.g. physicians, hospitals, laboratories, pharmacies, PBMs
- **Health Plans** - E.g. health insurers, payers, HMOs. Medicare etc.
- **Healthcare Clearing Houses** – E.g. billing Services, re-pricing companies etc.

Business Associates

- An entity or a person who performs certain functions or activities that involve the use, disclosure, maintenance, and/or transmission of PHI on behalf of a Covered Entity

Subcontractors

- An entity or person to whom a Business Associate delegates a function, activity, or service

What is Protected Health Information (PHI)?

Protected Health Information (PHI) is individually identifiable health information, including demographic data, that relates to an individual's physical or mental health (past, present or future).

PHI can be in *written, verbal or electronic formats* and includes:

1. Names
2. Street address, city, county, precinct, zip code, and equivalent geo-codes
3. All elements of dates
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan ID numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers/serial numbers
14. Web addresses (URLs)
15. Internet IP addresses
16. Biometric identifiers, incl. finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

Overview of HIPAA Security Rule

The **Security Rule** established standards that require covered entities to implement Administrative, Technical and Physical safeguards to protect electronic Protected Health Information (ePHI).

Key provisions include standards governing:

- Security Management Process, including Risk Analysis, Risk Management, Information Systems Activity Review, Sanctions Policy
- Assigned Security Responsibility
- Information Access Management
- Security Incident Procedures
- Security Awareness and Training
- Device and Media Controls
- Audit Controls
- Transmission Security

Overview of HIPAA Privacy Rule

The **Privacy Rule** sets the standards for how covered entities and business associates maintain the privacy of written, verbal or electronic Protected Health Information (ePHI).

Key provisions include standards governing:

- Rights of Privacy (to access, amend, copy, request restriction, request confidential communications, to an accounting of disclosures of PHI, etc.)
- Permitted Uses and Disclosures, including those requiring authorization
- Verification Requirements (i.e. prior to disclosing PHI to patients or third-parties)
- Business Associates Contracts
- Data De-identification and Re-identification
- Minimum Necessary
- Limited Datasets
- Policies and Procedures (including Notice of Privacy Practices)

HIPAA Breach Notification laws provide clear rules for notifying relevant parties following a breach of unsecured PHI and/or PII

HIPAA Breach Notification Rule

- The **Breach Notification Rule** requires organizations (under certain conditions) to notify individuals, regulators, covered entities, business associates, or media outlets when a breach to the privacy of PHI has occurred
- Key provisions of the rule include;
 - The **definition of a breach** as the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule
 - Certain **exceptions** for inadvertent disclosure between workforce members
 - Certain **post-breach risk assessment** to determine risk of compromise to PHI
 - Notification requirements
 - Mandates **business associates** to notify covered entity(s) following the discovery of a breach
 - Notice must be provided **within 60 days** from discovery of the breach
 - If **more than 500** individuals have been affected, notice through prominent media outlets must occur; this is in addition to individual notices

HIPAA Breach Notification Risk Assessment

A Breach is reportable unless the covered entity or business associate, as applicable, demonstrates “*that there is a low probability that the PHI has been compromised **based on a risk assessment** of at least the following factors*”:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated

Impact of HIPAA/HITECH & Omnibus Final Rule on Life Science Organizations (1 of 2)

Clinical Trials

- Prior to start of clinical studies, covered entities **must have** trial subjects sign;
 - An Informed Consent Form
 - HIPAA Authorization
- Data cannot be used for purposes outside the scope of the Authorization (secondary use) without additional authorization

Research Activities

- A covered entity **may not use or disclose** PHI for research, except in one of the following circumstances:
 - The individual has signed a written Authorization
 - An IRB has waived or altered the requirement for HIPAA Authorization
 - The covered entity has “de-identified” the data prior to its use or disclosure

Marketing & Sale Activities

- Covered entities must obtain an **individual's authorization** before using or disclosing PHI for marketing purposes
- Sale of PHI without an individual's authorization **is prohibited** according to HIPAA regulations

Impact of HIPAA/HITECH & Omnibus Final Rule on Life Science Organizations (2 of 2)



Business Associates

- **Business Associates** are individuals or entities who, on behalf of a covered entity, perform or assist in performance of a activity involving the use or disclosure of PHI
 - Examples include pharmaceutical manufacturers, medical equipment suppliers, EMR software vendors etc.
- **Business Associates Agreements** are required between Life Science Organizations and third parties/vendors;
 - Only required for third parties/vendors that creates, receives, transmits or maintains PHI on behalf of the Life Science Organizations
 - Describes permissible use/disclosure of PHI by third parties/vendors
 - Requires third parties/vendors to use appropriate safeguards to use or disclosure of PHI

Discussion on General Data Protection Regulation (GDPR)

Overview of GDPR

What is GDPR?

- GDPR stands for General Data Protection Regulation and aims at providing a uniform approach to managing data protection throughout the EU
- GDPR is set to be finalized in March 2016, with final implementation and required compliance by 2018

What type of data falls under GDPR?

- Personal data which is defined as data relating to an identified or identifiable person
 - E.g. - location data, online identifiers, genetic data and biometric data

What type of data falls outside of GDPR?

- Impersonal Data (Anonymized)
 - Personal Data is **irreversibly** anonymized only if it cannot be manipulated in any manner such that the individuals may be identified in any way from the data

Who will GDPR apply to?

- Any organization that is active in Europe will need to comply with the GDPR.
 - This includes organizations with no establishment in the EU but which are directing goods and services at people in the EU or are monitoring people there
 - GDPR extends the scope of the EU data protection law to all foreign companies processing data of EU residents

GDPR Key Points

GDPR promotes giving **data subjects an increased level of control over their information** and will make **consent much harder to obtain and prove**.

The GDPR also **increases accountability**, requiring companies to prove compliance with the regulation and giving **regulatory authorities increased oversight**.

Key points in the regulation:

- Privacy by design
- Right to be forgotten
- Breach of personal data penalties
- Potential for brand damage
- Data protection officer
- Citizens rights'
- Being a supplier (data processor)
- Proving compliance

GDPR in a Nutshell

Privacy by design

- Requires organizations to **consider privacy throughout the design of any new system, product, service or process**
- Requires entities to ensure that **personal data is used in a way that is in line with citizens' rights**
- Process the **minimum amount of personal data necessary** for a particular purpose

Right to be forgotten

- Right of data subject **to erase the data held by companies at any time**, including from any third parties

Breach of personal data penalties

- European Council may fine of up to **4% of the annual global turnover**

Potential for brand damage

- Entities will be required to report data breaches of the data subjects personal data or privacy to the regulators and to the individuals affected

GDPR in a Nutshell

Data Protection Officer (DPO)

- Inform and advise the organization of its obligations under the GDPR
- **Monitor compliance with the GDPR and requirements** relating to privacy by design, privacy impact assessments, data security and the rights of individuals

Citizens' rights

- These include for a data subject **to access their personal data**, to better **monitor and amend it**, and the right to **erase personal data** that is incorrect or no longer relevant
- Request the transfer of their personal data from one service provider to another service provider upon request, which is referred to as '**data portability**'

Being a supplier

- An **entity handling another organization's information** will now **be directly liable** under the GDPR **for failure to meet requirements**

Proving compliance

- **Perform and document privacy risk assessments and privacy audits** where the activity poses a specific privacy risk

Impact of GDPR on Life Science Organizations

A key requirement of the GDPR is that Privacy Impact Assessments (PIAs) are completed for all new processes, technologies, systems and devices, and PIA's with high risk are reported to the supervisory authority. Based on this requirement, key controls are likely:

Clinical Trials

- Controls indicated by the PIA are implemented, which may include:
 - Trial subjects provide consent
 - Processes to handle requests of the trial subject revoke consent or correct data
 - Strong controls established to prevent any secondary use of data

Research Activities

- Controls indicated by the PIA are implemented, which may include:
 - Research data subjects provide consent
 - Psuedoanonymization or real anonymization of data in the research data set
 - Strong controls established to prevent any secondary use of data retained for research purposes

Marketing & Sale Activities

- Controls indicated by the PIA are implemented, which may include:
 - Data subjects provide consent
 - Processes to handle requests to object to marketing activities are processed within 30 days
 - Processes to prevent secondary use, such as sale of personal information, without an individual's explicit consent

De-identified/pseudonymous data

HIPAA:

Safe Harbor

- Requires all 18 data types to be removed or modified (see slide 15). Researchers may claim that removing all 18 identifiers may limit the benefits of using health data for research and analysis

Expert Determination

- Requires an expert to assess the risk given the specific context for which the data will be used or released. Based on the level of risk, identifiers can be removed and modified so that the data remains useful for research and analysis, while still protecting privacy
- Currently, there are a limited number of experts who are trained to apply the Expert Determination methodology















GDPR:

Pseudonymous Data

- GDPR defines *pseudonymised data* as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information”.
- Data that falls into this category is subject to less rigorous restrictions than personal data
- Guidance for pseudonymised data will likely continue to evolve

Data Breach Enforcement Trends

The US currently leads enforcement, with EU enforcement likely to increase following the implementation of the GDPR² (General Data Protection Regulation).

Level 1 Country	Comprehensive Privacy Law?	Other Regulations	Data Covered	Enforcement body	Enforcement Fines	Enforcement Outlook
United States	No, sectoral privacy regulations and enforcement: FDA, FTC, HHS (HIPAA)	Device regulations (FDA), adverse event reporting	All consumer data	Yes		
Germany	Yes, based on EU Directive	EU Pharma-covigilance ³	All health-related information considered Sensitive Personal Information	Yes		
Netherlands	Yes, based on EU Directive	EU Pharma-covigilance ³	All health-related information considered Sensitive Personal Information	Yes		
UK	Yes, based on EU Directive	EU Pharma-covigilance ³	All health-related information considered Sensitive Personal Information	Yes		
France ⁴	Yes, based on EU Directive	EU Pharma-covigilance ³	All health-related information considered Sensitive Personal Information	Yes		
Canada	Yes, federal privacy law	Sectoral provincial regulations	Information about an identifiable individual	Yes		
Japan	Yes, privacy act contains general guidelines	Medical Devices Act	Information about an identifiable individual	No national DPA		



Trending towards increase



Potential to increase

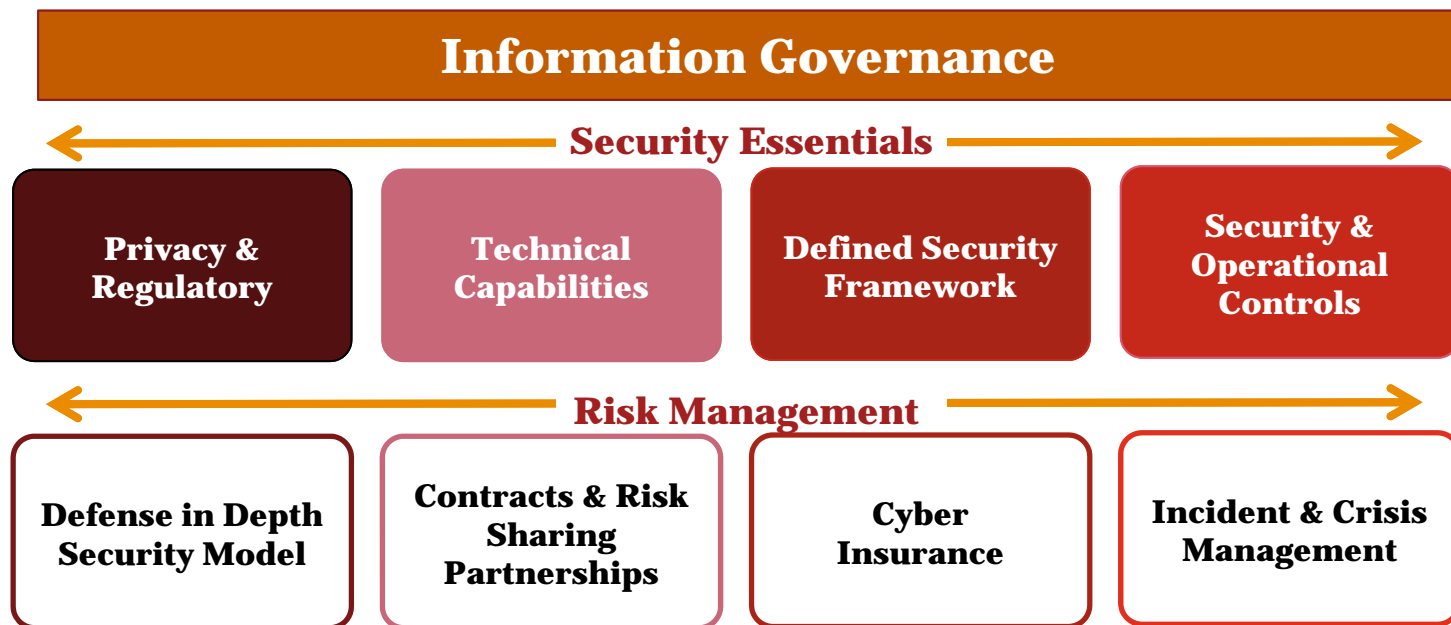


Emerging

¹List is not comprehensive ² Proposals under review include penalties of 100 million euro or to 2-5% of the annual worldwide turnover. https://www.huntonprivacyblog.com/files/2015/03/EU_Regulation_Guide_Overview.pdf ³ http://ec.europa.eu/health/human-use/pharmacovigilance/index_en.htm ⁴ Data localization required

Compliance in Practice

Technology is not enough – Compliance requires a combination of processes, controls, and ongoing monitoring to secure data and manage risk



Various initiatives & techniques can enhance the robustness of your privacy/security program

Technical Security Safeguards

- Implementing security measures and technologies to protect sensitive data
- These includes access, audit & integrity controls, entity authentication, transmission security etc.

Corporate Governance, Culture & Compliance

- Establishing governance models to best align privacy, security, compliance and risk management in the organization

Certification

- Leveraging a common security framework to achieve certifications from healthcare and IT security standards such as HITRUST, HIPAA, COBIT, NIST, PCI DSS etc.



Policy Compliance Review

- Identifying and analyzing existing gaps in privacy policies
- Developing recommendations to mitigate such gaps

Data Handling & Theft Risks

- Implementing safeguards and controls to prevent loss of sensitive data due to theft and mishandling

OECD Privacy Framework

- Provides guidelines for cross-border data transfer of personal data between organizations globally
- Focusses on the practical implementation of privacy protection through a risk management approach

Risk Assessment

- Assessing the impact and risks to the privacy of sensitive data stored, used and exchanged between information systems
- Conducting assessment s to meet relevant requirements of European Union (EU) data protection laws

Case Study

After an incident involving sensitive personal information, your leadership would like you to perform an evaluation of your privacy and security program(s).

Specifically, leadership is seeking recommendations to enhance its controls around privacy and data protection of personal information, and compliance with respect to applicable privacy and data protection laws.

They would like to know if a breach has occurred, and if so what regulations apply to your organization and what baseline controls your organization will be required to meet.

How would you approach this request?

Thank You!

For additional information or questions, please contact:

Peter Claude



Partner,
Pharmaceutical & Life Sciences
peter.claude@pwc.com
(415) 606-5024

Kenia Rincón



Director,
Healthcare Cybersecurity & Privacy
kenia.rincon@pwc.com
(718) 518-2794