A SENSIBLE APPROACH TO GLOBAL SECURITY AND DATA PRIVACY

Michelle Caswell, JD, Principal, Coalfire
Juan Carlos (JC) Palacio, Associate Privacy Counsel, Stryker

1

THE GLOBAL PRIVACY CHALLENGE

Navigating a Complex Web

2

HEALTHCARE IN AN INCREASINGLY CONNECTED WORLD

- More connectivity and sensitive health data means more risk of:
  - Reputational harm
  - Lost Revenue
  - Regulatory investigations
  - Data breaches, cyberattacks, patient safety concerns
  - Class action lawsuits
- Increasingly aggressive oversight and enforcement environment
  - Multiple US regulators prioritizing cybersecurity
  - EU GDPR Supervisory Authorities (up to €20 million or 4% global revenue)

"Our record year underscores the need for covered entities to be proactive about data security if they want to avoid being on the wrong end of an enforcement action"

OCR Director Roger Severino, Concludes All-Time Record Year for HIPAA Enforcement with $3 Million Cottage Health Settlement", February 7 2019

stryker COALFIRE

3

THE, WHO, WHAT AND HOW OF PRIVACY REGULATIONS

US Healthcare Organizations potentially face multiple pools of applicable privacy regulations:

United States:

- Federal Regulations: Different Agencies for different sectors
  - Health and Human Services (HHS), Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), etc.
    - Moreover, at the Federal level organizations must take into account external guidance (i.e., National Institute of Standards and Technology (NIST)—Cybersecurity Framework & Privacy Framework (Proposed Draft)
- Patchwork of State laws: California Consumer Protection Act (CCPA); Nevada Privacy Law (SB 220); New York Privacy Act.
  - Create consumer rights and business obligations greater than most current Federal regulations

European Union (e.g., GDPR) and a growing number of other non-US countries in Latin America (e.g., LGPD), Asia-Pacific (e.g., PRC Cybersecurity Law) and elsewhere: Omnibus privacy laws applicable to all Personally Identifiable Information or PII, regardless of sector, category of individual, or type of PII.

stryker COALFIRE

4

STARTING AT THE BEGINNING

Healthcare organizations are faced with the unique challenge of navigating a complex and diverse privacy landscape.

Where to start:

- Determine what privacy laws apply to your organization.
- Build a risked based model where each applicable regulations' most stringent requirements are set as the floor.
- Start building the program your organization needs.

stryker COALFIRE

5

GLOBAL PRIVACY

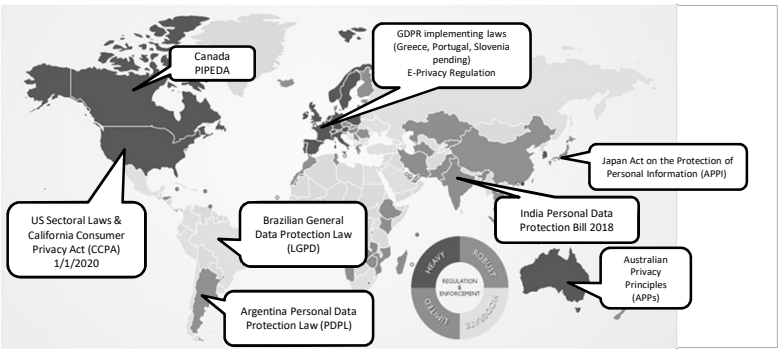
2019 Functional Insights

stryker COALFIRE

6

GLOBAL PRIVACY MANAGEMENT

Building a consistent approach



stryker COALFIRE

7

2019 AND BEYOND

For US Healthcare organizations, Protected Health Information is no longer the only game in town

Personal Information or PI is very broadly defined

Any data that can be linked to an identified or identifiable person

PI can to relate to employees, patients, customers, contractors, corporate customer contacts, distributor contacts, website visitors, business partner contacts, and other individuals

EXAMPLES:

- Name
- email address
- telephone number
- other contact information
- account information
- patient ID
- payment card information
- IP address

stryker COALFIRE

8

What Risk Looks Like for US Healthcare Organizations

9

stryker

COALFIRE

9

CALIFORNIA CONSUMER PROTECTION ACT (CCPA)

- Starting January 1, 2020, new privacy rights for California residents and new business obligations for organizations covered under the law.
  - Personal: right to request deletion of personal information, right to request disclosure of regarding the collection of personal information, right to opt-out of selling personal information to third parties, private right of action.
  - Business: Notice and Disclosure requirements, "Do Not Sell" button on website.
- The CCPA includes several **exemptions** that may permit health and life sciences companies to limit their compliance obligations or exempt their activities entirely.
  - Non-profit entities.
  - HIPAA covered entities and business associates.
  - Health care providers subject to CMIA.
  - Clinical trials subject to the Common Rule.

stryker

COALFIRE

10

WHAT IS GENERAL DATA PROTECTION REGULATION (GDPR)?

Applies to any organization that:

- has employees in the EU
- offers goods or services to EU residents (even if no payment is required)
- monitors behavior of an EU resident

- Applies to "personal data" of EU resident

stryker® COALFIRE.

11

WHAT ARE GDPR'S KEY DIFFERENCES FOR US COMPANIES?

US	GDPR
• *FTC*: "not yet linked to a particular consumer, computer, or device but that may ***reasonably*** become so" • *CaCPA: "identifies*, ***relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly***, with a particular consumer or household." • *State Data Breach Law:* first name or first initial with last name PLUS SSN, D.L./gov't ID card, bank account/ credit/debit card, or health insurance information. Some states: biometric data, health data. • *HIPAA*: Protected Health Information (18 identifiers)	Personal data is data "relating to an ***identified or identifiable natural person***; an identifiable natural person is one who can be identified, ***directly or indirectly***, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

stryker® COALFIRE.

12

WHAT ARE GDPR'S KEY DIFFERENCES FOR US COMPANIES?

- **Requires "lawful basis" for processing personal data**
- **Requires Data Protection Impact Assessment (DPIA) when "high risk" processing, e.g., when data is processed by new technology**
- **Requires Lead Supervisory Authority or Representative**
- ***May* require a Data Protection Officer (who has "expert knowledge," directly reports to "highest management level" and no conflict of interest) and/or Record of Processing**

stryker COALFIRE

13

WHAT ARE GDPR'S KEY REQUIREMENTS US HEALTHCARE ORGANIZATIONS SHOULD BE FAMILIAR WITH….

Rights of Data Subjects

- Right to Erasure (a.k.a. Right to be Forgotten) - Right to request erasure of personal data "without undue delay" if the data is no longer needed, the data subject objects to the processing or the processing was unlawful.
- Data Portability - Right to receive personal data processed through "automated means" in a commonly used and "machine-readable" format
- Right of Access - Right to know what personal data is processed and why
- Right of Rectification
- Right to Restrict Processing
- Right to Object to Processing

stryker COALFIRE

14

THINKING ABOUT RISKS BROADLY

Personal Data Breach

US	GDPR
Under state law, a breach is typically defined as "unauthorized acquisition of computerized data that compromises the **security**, **confidentiality**, or **integrity** of personal information." The **availability** of data is considered under HIPAA with respect to ransomware incidents.	• **Availability breach** ***Accidental or unlawful destruction or loss of personal data*** • **Integrity** breach *Alteration of personal data.* • **Confidentiality** breach *Unauthorized disclosure of, or access to, personal data.* … or a combination of these

stryker

COALFIRE

15

COUNTRIES WITH LAWS LIKE GDPR

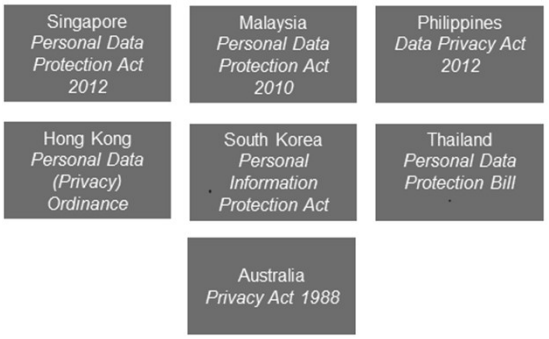
- **Countries with "adequacy determinations" (EU designation)**
  - Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and U.S. (limited to the Privacy Shield framework)
  - Japan – just announced
- Brazil – *NEW* - applies to the personal data of Brazilians regardless of the location of the entity collecting the data
- India – *PROPOSED*

stryker

COALFIRE

16

ASIAPAC COUNTRIES WITH DATA PROTECTION LAWS



stryker

COALFIRE

17

THE PRIVACY / SECURITY CONNECTION

Implementing Reasonable Security

stryker

COALFIRE

18

PRIVACY REGULATIONS' SECURITY REQUIREMENTS

HIPAA -

Covered entities and business associates are required to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or vulnerabilities to the security of EPHI.

GDPR -

"… appropriate technical and organisational measures to ensure a level of security appropriate to the risk

Canada – PIPEDA Principle 4.7 requires that personal information be protected by safeguards appropriate to the sensitivity of the information; PIPEDA Principle 4.7.1 requires security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

China's Personal Information Security Specification – a data controller must implement "*adequate*" technical and organizational measures to ensure data security. (Section 4)

stryker COALFIRE

19

WHAT IS REASONABLE SECURITY?

Flexibility of approach:

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

45 C.F.R. 164.306(b)(1)(2)

stryker COALFIRE

20

REASONABLENESS TAKES TEAMWORK

- Legal Representative(s)
- Privacy/Compliance Officer
- Security Officer/CISO/CIO
- IT Team
- Application Owners/Data Owners
- Incident Response team technical
- Incident Response team non-technical
- Facilities Director
- Network Architect/Security Architect

stryker

COALFIRE

21

NIST – RISK MANAGEMENT FRAMEWORK

A System Life Cycle Approach for Security and Privacy

1. Categorize Information Systems
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize Information System
6. Monitor Security State

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

stryker

COALFIRE

22

CATEGORIZE INFORMATION SYSTEMS

- Identify assets and information systems that create, receive, transmit, or maintain sensitive information
- The security controls applied should focus on these organizational operations and assets, individuals, or other organizations should there be a loss of confidentiality, integrity, or availability.

Resolution Agreement – Organization A – "As part of this process, A shall develop a complete inventory of all electronic equipment, data systems, off-site data storage facilities, and applications that contain or store ePHI which will then be incorporated in its Risk Analysis."

stryker

COALFIRE

23

SELECT SECURITY CONTROLS

- Selection of baseline security controls for each information system;
- Application of security control tailoring guidance for the information systems to allow organizations to adjust the initial security control baselines with respect to specific mission and business processes, determined during the security categorization process;
- Supplementation of tailored baseline security controls with additional controls based on an assessment of risk;
- It is important for organizations to document the decisions taken during the security control selection process, providing a sound rationale for those decisions.

Resolution Agreement – Organization B "B shall develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities identified in the Risk Analysis. The Risk Management Plan shall include a process and timeline for B's implementation, evaluation, and revision of its risk remediation activities."

stryker

COALFIRE

24

IMPLEMENT SECURITY CONTROLS

- Implement the security controls that have been determined to be reasonable and appropriate for the organization.
- Security control implementation employs enterprise architectures, the System Development Lifecycle (SDLC), and various NIST publications to guide the implementation of security controls in organizational information systems.

Reasonable is the key here – (ALJ granted summary judgment in favor of OCR) - "Respondent eventually determined that the mechanism with which it would protect confidential data including ePHI would be the encryption of the devices on which such data is stored. In 2008 Respondent announced that it intended to implement the first phase of a media security project that would test and implement encryption of institutional laptop and desktop computers. OCR Ex. 9 at 10. However, despite identifying the risk of and dangers related to confidential data loss and deciding on encryption of devices as a means of protecting data, Respondent delayed encryption of laptop devices for years and then, proceeded with encryption at a snail's pace."

stryker

COALFIRE

25

ASSESS SECURITY CONTROLS

- Evaluate the information system security controls for effectiveness using appropriate methods and procedures to determine the extent to which the controls are implemented correctly;
- Operating as intended; and
- Producing the desired outcome with respect to meeting the security objectives and requirements for the system.

Resolution Agreement – Organization C - Implement Process for Evaluating Environmental and Operational Changes - Organization C shall develop a written process(es) to regularly evaluate any environmental or operational changes that affect the security of ePHI in the Organization C possession or control ("Evaluation Process").

stryker

COALFIRE

26

AUTHORIZE INFORMATION SYSTEMS

Inherent in any risk management process is the acceptance of those identified risks that are deemed acceptable to the organization.

Resolution Agreement – Organization D - Organization D will within one-hundred fifty (150) days then incorporate the results of the Risk Analysis into its existing process for implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level as required by the Security Rule and will provide such documentation to HHS upon request.

stryker

COALFIRE

27

MONITOR SECURITY STATE

- Threats and vulnerabilities to an operating environment, as well as safeguards designed to combat them, can change frequently.
- The assessment and evaluation of security controls on a continuous basis provides oversight and monitoring of the security controls to ensure that they continue to operate effectively and as intended.
- Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the system security status to appropriate organizational officials on a regular basis.

Resolution Agreement – Organization E- “E shall review the Risk Analysis annually. E shall also promptly update the Risk Analysis in response to environmental or operational changes affecting the security of ePHI. Following an update to the Risk Analysis, E shall assess whether its existing security measures are sufficient to protect its ePHI, and revise its Risk Management Plan, policies and procedures, and training materials, as needed.”

stryker

COALFIRE

28

NIST NOW = NO REGULATORY ENFORCEMENT LATER?

- Due Diligence
  - What if you were proactive in your approach to privacy and security?
  - What if you took more than a checklist approach to privacy and security?
  - Could you respond to a request like this in 14 days?

1. A written detailed description as to what happened and how it happened (root cause). Please describe the manner in which [redacted] covered the breach.
2. A dated copy of [redacted] comprehensive, enterprise-wide risk analysis conducted prior to the incident, and a copy of any conducted after the incident, pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(A). The risk analysis should identify where all of the ePHI an entity creates, receives, maintains, or transmits is in order to understand the scope of the risk analysis. A risk analysis must address the potential risks and vulnerabilities that can affect all of your information systems or electronic media that processes or stores ePHI. The risk analysis must contain certain key elements, such as identifying and documenting the risks and vulnerabilities (including technical and nontechnical vulnerabilities), assessing and assigning a risk level for each risk, and documenting corrective actions to mitigate each risk. Please provide any and all documents showing evidence of the above.
3. A copy of [redacted] risk management plan that was created to reduce the identified risks in response to the risk analysis pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(B).
4. What types of network security controls are in place? E.g. Firewalls, Intrusion Detection Systems, web filtering, Data loss prevention, other security monitoring devices. 45 C.F.R. § 164.312(e)(1).
5. Copy of any and all procedures, implemented before the breach, to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 45 C.F.R. § 164.308(a)(1)(ii)(D).
6. Copy of any and all procedures related to the management of access to ePHI by employees who have been granted the authorization to do so. 45 C.F.R. § 164.308(a)(4)(i).

stryker

COALFIRE

29

SECURITY SIMPLIFIED

- Involve the 'right' team members
- Know what data is flowing in and out of your organization
- Maintain inventory of your assets
- Develop your organization's risk appetite
- Understand your legal obligations
- Perform 'non-technical' and 'technical evaluations'
- Stay up-to-date on the latest technologies
- Get involved in information security and privacy groups

stryker

COALFIRE

30

QUESTIONS?

- Michelle Caswell, JD, Principal, Coalfire – michelle.caswell@coalfire.com
- Juan Carlos (JC) Palacio, Associate Privacy Counsel, Stryker - juan.palacio@stryker.com

stryker®

COALFIRE.

31