How do International Laws & Regulations Intersect with HIPAA & Other US Laws & Regulations?

MarK Steinhoff
Managing Director, Privacy & Data Protection
Deloitte & Touche, LLP

Angel Hoffman
Owner/Principal
Advanced Partners in Health Care Compliance, LLC
Agenda

• Understanding how global privacy requirements affect healthcare organizations in the United States
• The new European Union General Data Protection Regulation (EU GDPR)
• Understanding what the GDPR requires in action
• How to demonstrate effective compliance
• Questions / discussion
What is the pertinence of global privacy to healthcare organizations in the United States?
The globalization of healthcare is a driving force

• Healthcare organizations are no longer located in singular jurisdictions

• Healthcare organizations are providing more far reaching services
  ▪ Specialty services
  ▪ Referrals
  ▪ Destination medicine
  ▪ Clinical trials

• Privacy is more than just the Health Insurance Portability and Accountability Act (HIPAA)
  ▪ Federal e-marketing
  ▪ State SSN and health privacy
  ▪ Federal and State Data Breach

• Global privacy specific to residents of a given jurisdiction
  ▪ Cross-border transfer of personal data and sensitive personal data
  ▪ Requirements for notice, choice, unambiguous voluntary consent, access and erasure
Let’s face it, privacy was already complex

Canada
- Federal/Provincial
  - PIPEDA, FOIPPA, PIPA

US Federal
- HIPAA
- Genetic Information Non-Discrimination, Privacy Shield
- CAN-SPAM
- COPPA

US Numerous State Laws
- Breach Notification | SSN
- State Security Laws
- State Health Privacy Laws

Mexico
- Federal Data Protection Act

Brazil
- Draft Data Protection Bill

Chile
- Law for the Protection of Private Life

Argentina
- Personal Data Protection Law, Confidentiality of Information Law

Europe
- European Union
  - EU Data Protection Directive
  - EU General Data Protection Regulation
  - United Kingdom - Data Protection Act 1998
  - United Kingdom - Privacy and Electronic Communications Regulations 2003
  - Germany - Data Protection Act
  - Germany - Work Constitution Act
  - Spain - Royal Decree Approving Regulation Implementing Organic Law On The Protection of Personal Data and various other member states data protection laws

Russia
- Personal Data Act 2006 Amended 2009, other requirements

Hong Kong
- Hong Kong Personal Data Privacy Ordinance

China
- Tort Liability of the Republic of China
- Privacy Law
- Cyber Security Law

Japan
- Personal Information Protection Act
- Basic Policy on Protection of Personal Information

India
- Data Privacy Rules 2011

In South Korea
- Act on Promotion of Information and Communications Network Utilization and Data Protection

Taiwan
- Computer-Processed Personal Data Protection Law

Australia
- Federal Privacy Amendment Bill
- State Privacy Bills in Victoria, New South Wales and Queensland, new e-mail spam and privacy regulations

South Africa
- Protection of Personal Information Act

Singapore
- Personal Data Protection Act

New Zealand
- Privacy Act 1993 Amended 2008

China
- Tort Liability of the Republic of China
- Privacy Law
- Cyber Security Law

India
- Data Privacy Rules 2011

South Korea
- Act on Promotion of Information and Communications Network Utilization and Data Protection

Taiwan
- Computer-Processed Personal Data Protection Law

Australia
- Federal Privacy Amendment Bill
  - State Privacy Bills in Victoria, New South Wales and Queensland, new e-mail spam and privacy regulations

South Africa
- Protection of Personal Information Act

Singapore
- Personal Data Protection Act

New Zealand
- Privacy Act 1993 Amended 2008

China
- Tort Liability of the Republic of China
- Privacy Law
- Cyber Security Law

India
- Data Privacy Rules 2011

South Korea
- Act on Promotion of Information and Communications Network Utilization and Data Protection

Taiwan
- Computer-Processed Personal Data Protection Law

Australia
- Federal Privacy Amendment Bill
  - State Privacy Bills in Victoria, New South Wales and Queensland, new e-mail spam and privacy regulations

South Africa
- Protection of Personal Information Act

Singapore
- Personal Data Protection Act

New Zealand
- Privacy Act 1993 Amended 2008
A typical complex privacy operating environment for a global organization

Ilustrative Privacy Regulatory Landscape

Canada
- Quebec Privacy Act
- Canada - PIPEDA
- Canada - PIPITPA
- Canada - CASL

United States
- HIPAA Privacy & Security Rule
- Genetic Information Nondiscrimination Act
- Telephone Consumer Protection Act
- CAN-SPAM
- California Civil Codes
- California Online Privacy Protection
- Connecticut Confidentiality of Social Security Numbers
- Massachusetts Regulations
- Texas Identify Theft Act
- Texas Health and Safety Code

Latin America
- Mexico - Federal Law on the Protection of Personal Data
- Argentina - Regulation 60 (DNPD Disposition 60)
- Argentina - Data Protection Law 2000
- Brazil - Data Protection Bill of Law No. 5276/2016

EMEA
- Netherlands - Dutch Notification of Data Breach Law
- Germany - Federal Data Protection Act & Works Constitution Act
- Spain - Royal Decree 1720-2007
- Italy - Personal Data Protection Code
- European Union - General Data Protection Regulation (GDPR)
- European Union - e-Privacy Directive

APAC
- Singapore - Personal Data Protection Act 2012
- India - Privacy Rules 2011
- Philippines - Data Privacy Act of 2012
- Australia - Federal Privacy Act 1988

Copyright © 2017 Deloitte Development LLC. All rights reserved.
Defining personal information in a global environment (partial example)

Personal information ("PI") is generally defined as *information relating to an identified or identifiable natural person (meaning directly identifiable or inferred)*. This could include individuals such as job applicants, employees, contingent workers, former employees, retirees, patients, healthcare providers, caregivers, dependents, contractors, consultants, suppliers, customers, etc.

<table>
<thead>
<tr>
<th><strong>Personal Information / Business Contact PI</strong></th>
<th><strong>Employment PI</strong></th>
<th><strong>Financial Account Related PI</strong></th>
<th><strong>Identification PI / Regulated Data</strong></th>
<th><strong>Sensitive PI</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name</td>
<td>• Work address</td>
<td>• Financial account information</td>
<td>• Date of birth</td>
<td>• Race</td>
</tr>
<tr>
<td>• Job title</td>
<td>• Work email address</td>
<td>• Password/PINs</td>
<td>• Mother’s maiden name</td>
<td>• Ethnic origin</td>
</tr>
<tr>
<td>• Work phone number</td>
<td>• Professional qualifications</td>
<td>• Driver license number</td>
<td></td>
<td>• Gender</td>
</tr>
<tr>
<td>• IP Address</td>
<td>• Photograph</td>
<td>• National identifier (e.g., SSN)</td>
<td></td>
<td>• Religious beliefs or affiliations</td>
</tr>
</tbody>
</table>

The types of personal information, sensitive personal information and regulated information varies by industry and geolocation.
Privacy requirement commonalities

There exists a high degree of commonality across privacy requirements, which can be broadly summarized into the following categories (aka domains):

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement Commonalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Includes requirements to establish management accountability and responsibility for privacy and the specific organizational roles and responsibilities for legal entities and/or individuals. The category also includes obligations to train employees, define, document and communicate privacy policies and procedures and notify, register, and/or file processing activities with local DPAs.</td>
</tr>
<tr>
<td>Notice</td>
<td>Includes requirements to notify and disclose to data subjects details of the organization’s data privacy practices including how data subjects’ information is protected and the purposes for which their personal information is collected, used and disclosed. Such requirements include the presentation of privacy notice prior to the collection of personal information as well as those surrounding the form and content of such notice.</td>
</tr>
<tr>
<td>Choice</td>
<td>Includes requirements to obtain consent from data subjects or to otherwise provide choice, for the use of personal information for primary or secondary purposes. Such requirements include those surrounding the form and content of the consent provided by the data subject, consent revocation procedures as well as opt-out and opt-in process management.</td>
</tr>
<tr>
<td>Access</td>
<td>Includes requirements to permit data subject’s access to personal information that the organization may have about them. Closely tied to these requirements are the data subject’s right to amend incorrect details and to reasonably request the deletion of unauthorized, unnecessary or inaccurate information subject to certain exceptions. Such requirements include the rights of data subjects to request, obtain, rectify, update and, when applicable, suppress or keep confidential their information.</td>
</tr>
<tr>
<td>Security for Privacy</td>
<td>Includes requirements to provide administrative, technical and/or physical security controls to prevent unauthorized or accidental loss, corruption or disclosure of personal information related to data subjects. Such requirements include those surrounding the development and implementation of written information security policies and procedures as well as implementation of physical and electronic access controls, transmission controls, monitoring controls, availability controls and third-party controls.</td>
</tr>
<tr>
<td>Transfer</td>
<td>Includes data protection requirements for the transfer of personal information to third parties or to other countries. Such requirements include the identification of current data transfers, the security of the transfer, compliance with local registration requirements, and documented business need for the transfer of personal data.</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Includes requirements that relate to the quality of information the organization has about its data subjects. Such requirements include those related to the organization’s efforts to confirm that personal information collected, used or disclosed by or on behalf of an organization is relevant, accurate, complete, and up-to-date.</td>
</tr>
<tr>
<td>Information Mgt</td>
<td>Includes data protection requirements on the collection, use, storage and destruction of personal information. Such requirements include those surrounding the manner in which and purpose for which data is obtained, the retention period of such data, the use of such data as it relates to the purpose for which it was obtained or the manner in which such data is deleted, made anonymous or returned.</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>Includes requirements which provide specific notification procedures in the event of a privacy/security breach. Includes those surrounding breach assessment and the need for notification as well as timing, form, content and distribution of the notification.</td>
</tr>
</tbody>
</table>
Let’s take one example

The new European Union General Data Protection Regulation (EU GDPR)
And things are going to get more interesting

“Safe Harbor” mechanism of “Cross Border Data Transfer” invalidated by the EU Court of Justice
October 6, 2015
Replaced by “Privacy Shield”
July 12, 2016

EU “Trilogue” agreed to the final text of the new GDPR
December 15, 2015
Regulatory Compliance Date
May 25, 2018

- Game changers in the execution of corporate and global privacy programs
- Require significant efforts to demonstrate compliance
- Potential for far-reaching impacts
Overview of the EU GDPR
The GDPR ushers in vast changes to the privacy landscape

The regulation in numbers

After four years of negotiations, the EU General Data Protection (GDPR) is upon us and due to be enforceable on May 25, 2018. The new law will introduce a range of requirements that will have significant impacts on organizations. Combined with increasing demands from consumers, privacy has suddenly shot to the top of the corporate agenda. Below are just of the some notable figures that demonstrate the impact of the GDPR – the main headline being a maximum monetary penalty of 4% of annual global turnover that can be imposed in cases of serious non-compliance.

- 4% Potential fines as a percentage of global turnover
- 72 Hours given to report a data breach
- 250m Cost of 4% fine for a typical FTSE 100 company
- 28,000 Estimated number of new Data Protection Officers required in Europe (IAPP study 2016)
- 190+ Countries potentially in scope of the regulation
- 80+ New requirements in the GDPR
**Specific Changes in How Europe Protects Privacy**

The GDPR introduces many cutting-edge protections

<table>
<thead>
<tr>
<th>Enlarged scope and applicability</th>
<th>Increased data subject rights: e.g., right of erasure and data portability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory Data Protection Officer</td>
<td>Introducing data breach notification</td>
</tr>
<tr>
<td>Focus on accountability (e.g., controllers / processors) &amp; transparency duties</td>
<td>Major strengthening and alignment of enforcement powers and sanctions</td>
</tr>
<tr>
<td>Privacy by Design/Default and Privacy Impact Assessments required to be embedded</td>
<td>Increased advisory &amp; enforcement cooperation between Data Protection Authorities</td>
</tr>
</tbody>
</table>
The GDPR has new requirements that may be tricky for organizations to address.

**Compliance Challenges**

- **Third-Party Risk Management**
  The GDPR lists clear requirements for data processors. Organizations may need to renegotiate third-party contracts to enable compliance.

- **Increased Recordkeeping**
  Organizations will have to identify and inventory processes and systems handling personal information.

- **Data Access**
  Data subjects have the right to be forgotten, and can even request that their data be transferred to competitors.

- **Transparency**
  Clarified transparency requirements require update of many privacy notices and statements.

- **Breach Notification**
  Will be challenging for entities to understand the nature of an incident within the 72-hour window, which may lead to premature engagement with regulators.

- **Data Privacy Impact Assessments**
  Organizations may have to allocate significant resources to develop an effective assessment program.
Questions being asked and how companies are gauging their current state
Are you prepared to answer the questions?

Who’s asking?

- Privacy
  - How are your peers attempting to comply?
  - Can you provide a compliance roadmap?
  - Can you build a case to leadership for resources?

- Legal
  - What are the pertinent regulatory requirements? How different are the requirements of the GDPR compared to our existing requirements?

- IT & Info Sec
  - What responsibilities will IT & Info Sec have to comply with the GDPR?
  - Do I have the resources to enhance and maintain the IT programs under the expanded regulations?

- Compliance & IA
  - What responsibilities will Compliance have under the GDPR?
  - How are clients managing the administration of Privacy Impact Assessments (PIA)s?

What’s being asked?

Compliance mechanisms

- Broad privacy gap assessment, including the GDPR
- IT-focused GDPR gap assessment
- GDPR-focused gap assessment
- Vendor Risk Support
- PIA Support
- Gap Remediation Support
- Design & Build
- Data Flow Maps
- GDPR Compliance Roadmap
- Privacy Governance

Copyright © 2017 Deloitte Development LLC. All rights reserved.
What questions are being asked?
If your organization has a presence (brick and mortar) of consumers/customers (virtual operations) in the EU, the GDPR likely applies to you.

<table>
<thead>
<tr>
<th>Potential Question:</th>
<th>Who could be asked?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who is accountable for your GDPR compliance efforts?</td>
<td>Privacy, Legal, and IT</td>
</tr>
<tr>
<td>How has the C-suite responded the potential for fines being imposed by the GDPR?</td>
<td>Privacy</td>
</tr>
<tr>
<td>How are you planning for the requirements of the GDPR?</td>
<td>Privacy, Legal, Compliance, and IT</td>
</tr>
<tr>
<td>Do you have an inventory as to where your personal data is? What about within your</td>
<td>Privacy, Business teams, and IT</td>
</tr>
<tr>
<td>“shadow IT” environment? Transfer?</td>
<td></td>
</tr>
<tr>
<td>Do you know which of your third-party vendors have your data? What about past</td>
<td>Privacy, Business teams, and IT</td>
</tr>
<tr>
<td>vendors? Do you conduct pre-contract assessments? Do you audit as a routine?</td>
<td></td>
</tr>
<tr>
<td>Where are you imbedding the PIA process within your operations? Who is leading the</td>
<td>Privacy and IT</td>
</tr>
<tr>
<td>associated remediation?</td>
<td></td>
</tr>
<tr>
<td>How are you preparing to respond to requests from a consumer to delete their records?</td>
<td>Privacy and IT</td>
</tr>
<tr>
<td>What about access and provisions in an electronic format?</td>
<td></td>
</tr>
<tr>
<td>How confident are you that the organization can meet the 72-hour breach notification</td>
<td>Privacy and IT</td>
</tr>
<tr>
<td>requirement?</td>
<td></td>
</tr>
<tr>
<td>Do your data mining activities comply with the GDPR’s requirements? Do you use</td>
<td>Privacy, Legal, Business teams, and IT</td>
</tr>
<tr>
<td>automated methods to make decisions without human intervention?</td>
<td></td>
</tr>
</tbody>
</table>
How mature is your privacy program?

The diagram below illustrates a privacy program maturity model that can be used to review and assess the current maturity of a privacy program. The information provided within this diagram are illustrative activities that occur under associated maturity ranking across domain components.

Privacy Program Maturity Model

- **Ad Hoc**
  - Procedures or processes are generally informal, incomplete, and inconsistently applied.

- **Repeattable**
  - Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.

- **Defined**
  - Procedures and processes are fully documented and implemented, and cover all relevant aspects.

- **Managed**
  - Reviews are conducted to assess the effectiveness of the controls in place.

- **Optimized**
  - Regular review and feedback are used to confirm continuous improvement towards optimization of the given process.

Source: AICPA Generally Accepted Privacy Practices (GAPP)
Demonstrating effective compliance
Demonstrating effective compliance

Privacy by design
- Consider privacy at start of process
- Account for end-to-end data lifecycle
- Consider context
- Define and implement privacy enhancing controls
- “Right to be forgotten”

PIA Process
- Prior to processing
- High-risk / sensitive data / systematic / large-scale
- Description, assessment, measures taken

Privacy by default
- Adopt privacy friendly settings (e.g., no pre-ticked box)
- Minimum storage time & volume
- Strictly necessary purposes only
Suggestions and considerations

- Identify and empower an individual within your organization to be the contact point (internal, external, regulatory) on Safe Harbor and GDPR to monitor, report and plan for changing legal obligations and establish consistent messaging.
- Gather existing documentation on data processing operations, including data transfers, to evaluate risk exposure and prepare for potential inquiries from DPAs, clients or employees.

- Develop an inventory of systems, controls, and procedures to understand where personal data are processed and which specific controls (e.g., data usage) exist.
- Assess available cross border transfer methods and select the method(s) that meet the requirements of your organization.
- Assess your current state (e.g., compliance with existing and new GDPR requirements, data processing registrations, third party sharing).

- Communicate regulatory changes and their potential impact to senior stakeholders to raise awareness and obtain senior-level support.
- Develop and implement a risk based remediation strategy and roadmap including a short-term tactical plan focusing on “quick wins”.
- Develop and execute a Works Council and DPA communications plan where appropriate.
Questions / discussion
How do International Laws & Regulations Intersect with HIPAA & Other US Laws & Regulations?

Angel Hoffman
Owner/Principal

Advanced Partners in Health Care Compliance, LLC
Objectives

• Describe the global privacy environment

• Discuss the potential requirements for the U.S. health care industry to meet the standards for privacy in the EU

• Identify other industries in the U.S. in addition to the health care industry required to follow GDRP

• Identify other U.S. laws
U.S. and Privacy

- U.S. Recognized need in 1974 for privacy and finally in 1996 HIPAA was created

- Not until 2003 and 2005 did privacy and security rules, respectively, become effective

- When U.S. consumers think of HIPAA, they often think that it covers all of their privacy rights. However, HIPAA only addresses those rights as they relate to Protected Health Information (PHI) transferred in any medium.
International Laws

• Many countries instituted privacy laws prior to HIPAA.
• There are differences between countries in how privacy is perceived and on the value placed on privacy of health data
• Privacy of health data is increasingly being recognized as an international value.
• Becoming familiar with the laws of various countries is critical for conducting international business to avoid violations.
• Whether conducting domestic international business, companies need to know what is addressed in each law and then conduct business accordingly to mitigate the risk of privacy breaches.
The European Union (EU)

- Has historically been more protective of personal information than the United States.
- One of the earliest and most recognized agreements and legislation supporting the transfer of health data across their borders was created by the EU in 1995.
- It passed a comprehensive data privacy law titled the, “EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.”
- The EU selected a “directive” approach that required each EU member state to enact its own law, based on the directive.
- As each EU member state developed and implemented its legislation, it implemented the 1995 rules differently, which resulted in divergences in enforcement and other related problems.
What does this mean for U.S. Companies?

Plain and Simple…

You need to have and understanding of each country and their interpretation of the EU directive.

Not so easy is it?
General Data Protection Regulation (GDPR)

• In late 2015, the EU’s GDPR was enacted to provide consumers with more input about how their digital information was collected and managed.

• This strengthened the privacy rights of Europeans.

• The changes took effect in early 2017 across the 28 members of the EU.

• One of the unique concepts in the GDPR is the “right to be forgotten,” which provides individuals in a region the right to ask companies to remove data about them.

• The law also requires companies to inform national regulators within three days of any reported data breach.

• This goes beyond what is required by U.S. authorities currently.
Other GDPR issues

• Children under 16 years old - The rule requires young children to obtain parental consent before using popular internet services, such as social media applications.
• In early 2016, the EU and the United States agreed to a framework for data sharing.
• The new framework is to protect the more stringent rights of EU citizens when their data is sent to the United States.
• It also includes safeguards and opportunities for redress should personal data be compromised.
Other U.S. Regulations

**FACTA - Fair and Accurate Credit Transactions Act**

To help protect consumers’ credit information from the risks related to data theft.

- Pursuant to FACTA, credit card and debit card receipts, with the exception of handwritten receipts, should not list more than the last five digits of the card number.
- It should be also noted that, under FACTA, a person making a request for a credit report has the right to request that the first five digits of his Social Security number not be included on the file.

**COPPA - Children’s Online Privacy Protection Act**

To protect the privacy of children under the age of 13.

The scope of the Act encompasses websites that are directed at children or that have knowledge that children are visiting the website.

COPPA imposes an obligation on the operators of these websites to publish privacy policies specifying whether or not personal information is being collected, how this information is being used, as well as the disclosure practices of the operators of the websites.

In order to collect this information from children, the websites’ operators must obtain verifiable parental consent.
Other International Agreements

• In addition to the EU, a number of other countries have developed international agreements and legislation related to privacy of personal data.

• What does not exist at this point is a single set of standards, rules, or legislation that could be used in designing information systems storing health-related data.

• Although both EU and Canada show evidence of being progressive in that direction, other countries have adopted privacy standards (e.g., Philippines in 2011, Vietnam in 2008, and South Africa in 2002).

• Find a list of these countries at:

Additional Information

• Informaticians should approach each international situation on an individual basis.
• Both the Electronic Frontier Foundation (EFF) https://www.eff.org/issues/international-privacy-standards and
• The Electronic Privacy Information Center https://epic.org/privacy/intl/ maintain websites listing privacy-related international agreements.  

Note: Neither list is comprehensive, but can be used as a starting point to explore international privacy agreements relevant to the privacy of health-related data.
Security Threats

Health care data is increasingly attractive to health data hackers.

Why?

• The expanding volume of healthcare data being stored
• Proliferation of EHRs interconnected by HIEs
• The internet of things (IoT)
• Recent health practices and the risk of a security breach, with the increased accessibility to electronic data and the transmission of data with the use of mobile devices
• Expanded health data sharing within and across health organizations
The Sharing of Health Data

• EHR information is no longer tied to one institution,

• Traditional stakeholders are transitioning to patients inputting information in their own records.

• HIE, by design, is meant to enable data sharing within a region and between regions.

• As population-based research is grows, so does the need for increased security for “big data”.

• Information is being published regarding how to share health data nationally and internationally.

• Increased risk of health data breaches
External Criminal Attacks

2015 was quite the year for health care data breaches.

• One reason is that stolen medical identity can be worth 10 to 20 times the value of a stolen credit card number.
• Criminals may use a stolen medical identity to obtain expensive health services or equipment that they can sell on the black market.
• It may take months or years for victims to learn that their medical identity has been compromised.
• Health care professionals must be aware that they are targets of attack from cybercriminals, simply due to their access to PHI.
How Wanacry Held the UK Health System Hostage

• The British newspaper The Guardian reported that the electronic system of the national health system "NHS" was subjected to systematic penetration caused by major technical problems.

• Hospitals and clinics in cities and counties in Britain, including the capital London, were unable to access a patient's personal database.

• All of the patient data had been encrypted by hackers demanding payment for the removal of the encryption system.

• To date there is no evidence to indicate the success of hackers in stealing patient and employee data.
External Threats Are Greater Than Internal Ones

• Today, one approach is for the industry to proactively consider the ethical, social, and legal implications in the design of innovative technologies.

• An example of this can be seen in the “Guidelines for Personalized Health Technology Final Report” developed under the direction of the Vitality Institute [http://thevitalityinstitute.org](http://thevitalityinstitute.org)
Vitality Institute Guidelines

These guidelines seek to build collaboration across the public and private sectors. The guidelines are built around five critical principles:

1. Build health technologies informed by science
2. Scale affordable health technologies
3. Guide interpretation of health data
4. Protect and secure health data
5. Govern the responsible use of health technology and data
Some banks are concerned about meeting GDPR obligations in time

- Concerns about meeting the forthcoming EU General Data Protection Regulation
- How to update legacy IT systems to meet the obligations set out by the GDPR
- Chief Technology Officers at banks, are concerned the technical challenge may be impossible given there is only a year to go.
- At some banks, a customer's data may be held on more than 100 systems, and each of these takes a long time to change, even for a simple change.
- Conflicting regulatory laws will complicate matters by potentially restricting what data can be shared or disclosed in the event of a cyberattack

© 2017 Advanced Partners in Health Care Compliance, LLC
What Are the Rules?

• Any American company that does business in the EU needs to be in full compliance with GDPR by May 25th, 2018.

• Even if your company has no presence in the EU, so long as you market to EU residents, even if it is through the web, you need to comply with the GDPR.

• Europe applies a much stricter standard for what is considered personal data than in the U.S. (e.g. anything outside of PHI does not fall under HIPAA)

• The cost of non-compliance could be devastating, and even fatal to many companies as you can be fined up to 4% of global annual revenue or €20 million, whichever is highest.

• The amount of the fine will be influenced by the nature, gravity and duration of the infringement.
What About Brexit?

• The question about the UK and Brexit is mostly interpreted as that GDPR will be applicable in the UK at least for the short and medium term.

• If your European establishment is in the UK only or if you only have UK clients in Europe, you should follow the evolution of Brexit and GDPR closely.

• Consumers care deeply about the abuse and loss of their data.
Steps to Prepare

• The first step is to understand the impact of GDPR on your organization

• Form a team comprised of business, legal, and IT specialists with enough authority to drive the complete change program.

• The sponsorship, program charter, and governance is led by a C-level executive, to give it the appropriate attention.
For each GDPR related change

• A decision needs to be made, if it has to apply to EU individuals only or if you should apply it to everyone.

• The latter is probably simpler technically as it reduces complexity and avoids the problem of determining individual applicability, but limit implementation of “right to be forgotten” to EU residents as it could be in conflict with US laws and the first amendment of the U.S. Constitution.

• It can also be less desirable from a business standpoint and in some cases be in conflict with laws in other countries.
Data breaches

• In terms of protecting EU citizens from data breaches, the survey found companies do not currently have the processes or technology in place to adequately meet GDPR requirements around data breaches.

• Only 52% of all of the companies surveyed are completely confident that they can report data breaches within 72 hours of discovery to the authorities.

• Only 55% are “completely confident” they have systems that could identify a breach from an external source, suggesting that a customer’s personal identifiable information could be traded unbeknown to the company or citizen, placing both at greater risk of fraud.
Data breaches (cont’d)

• Less than half (46%) are completely confident that they could precisely identify the data that had been exposed in a breach.

• GDPR regulations also state that “appropriate technical and organizational measures” should be in place to safeguard personal data and minimize data collection, processing and storage.

• Just over a third (37%) of companies claim to have processes that allow them to remove data without delay from live systems and backups.

• Articles 16 and 17 of the EU GDPR specify the companies must be able to respond to citizen demands for the rectification or erasure of data in one month (15% are currently building the systems that will give them this functionality).
## The EU vs. The U.S.

<table>
<thead>
<tr>
<th>EU Law</th>
<th>U.S. Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Under EU law, personal data can be collected only under strict conditions and for a legitimate purpose.</td>
<td>• In the US, there is no all-encompassing law regulating the collection and processing of personal data.</td>
</tr>
<tr>
<td>• The main component of the EU data protection law is the Data Protection Directive 1995/46/EC.</td>
<td>• Instead, data protection is regulated by many state and federal laws.</td>
</tr>
</tbody>
</table>
Where Are You in the Process?

• Process to legitimize the cross-border transfer of personal data, implementing privacy by design.

• Conducting privacy impact assessments, and preparing for compliance with 72-hour breach notification requirements, among other compliance challenges.

• Penalties for non-compliance under the GDPR, which is driving increased attention to and investment in privacy compliance readiness.
QUESTIONS AND DISCUSSION