What Every Lab Needs to Know About GDPR

Marty Barrack, SVP, General Counsel & Chief Compliance Officer | XIFIN, Inc.
How Labs Must Respond to Meet New Data Privacy Requirements
Agenda

- Review of Privacy Regulation Framework
- General Data Protection Regulation (GDPR) Basics
- General Privacy Trends and New State Laws
- Preparing for GDPR and the Future
Federal law takes a “sectoral” approach, regulating privacy within the federal government, state governments and otherwise on a subject matter basis.

For example:

<table>
<thead>
<tr>
<th>Health information:</th>
<th>HIPAA: privacy, security, breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="https://www.hhs.gov/hipaa/index.html">https://www.hhs.gov/hipaa/index.html</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Substance abuse information:</th>
<th>Substance Abuse and Mental Health Services Administration (SAMHSA) regulations applicable to Part 2 Programs:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs">https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Student records:</th>
<th>Family Education Rights and Privacy Act (FERPA)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Cell phone records:</th>
<th>Telephone Consumer Protection Act (TCPA)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Debt Collection:</th>
<th>Fair Debt Collection Practices Act (FDCPA)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Children’s privacy:</th>
<th>Children’s Online Privacy Protection Act (COPPA)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Privacy policy violations:</th>
<th>Section 5 of the FTC Act</th>
</tr>
</thead>
</table>
Data Privacy Regulatory Framework – State Law

Each state has its own data privacy laws

- All 50 states have enacted security breach notification laws

- Many states have enacted complex data privacy laws. For example:
    - Protects personal information, including social security, drivers license and other account numbers, and even a biometric indicator when combined with an individual’s name
    - Requires a Written Information Security Plan for the protection of Personal Information of MA residents
    - Requires breach notification
    - Regulations require specific IT practices,
  - California: California Consumer Privacy Act (more later)
    - An amazing patchwork of regulation: [https://oag.ca.gov/privacy/privacy-laws](https://oag.ca.gov/privacy/privacy-laws)
Data Privacy Regulatory Framework – Local Laws

Cities and other local governments can have their own data privacy laws

For example:
• Privacy First Policy, San Francisco
International laws follow a similar structure to laws in the United States, but can be more complex and are usually more protective of personal information:

- **Regional laws**: such as the European Union
  - 28 countries
  - Plus 3 additional countries in the European Economic Area

- **Country laws**
  - Each country in the EU has its own laws that must be consistent with EU law

- **Local laws**
  - Provinces, cities and other local governments can have their own laws
Reach of Data Privacy Laws

• Privacy laws may be limited by subject or scope
  – HIPAA:
    • Covered Entities:
      – health plans
      – health care clearinghouses
      – health care providers who electronically transmit any health information in connection with a HIPAA transaction
    • Protected health information

• Privacy laws may be limited by geography
What Is the GDPR

General Data Protection Regulation

• European data protection law effective May 25, 2018
• Applies to all countries in the EU/EEA:
  – 28 countries of Europe: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
  – 3 additional countries in the EEA but not in the EU: Iceland, Liechtenstein and Norway
  – https://www.gov.uk/eu-eea
• Biggest change in privacy laws in 20 years: revolutionary changes with substantial penalties for violation
• Text of GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Does it apply to you?
Territoriality of GDPR

Article 3 of the GDPR

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   a) The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   b) The monitoring of their behavior as far as their behavior takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.
Territoriality of GDPR - 2

When the regulation does not apply

“Your company is service provider based outside the EU. It provides services to customers outside the EU. Its clients can use its services when they travel to other countries, including within the EU. Provided your company doesn't specifically target its services at individuals in the EU, it is not subject to the rules of the GDPR.”


➢ Do you specifically target services at individuals in the EU?
“Example 2: An e-commerce website operated by a company based in China, whereas the data processing activities of which are exclusively carried out in China, has established a European office in Berlin in order to lead and implement commercial prospection and marketing campaigns towards EU markets. In this case, it can be considered that the activities of the European office in Berlin are inextricably linked to the processing of personal data carried out by the Chinese e-commerce website, insofar as the commercial prospection and marketing campaign towards EU markets notably serve to make the service offered by the e-commerce website profitable. The processing of personal data by the Chinese company can therefore be considered as carried out in the context of the activities of the European office, as an establishment in the Union, and therefore be subject to the provisions of the GDPR as per its Article 3(1).”

“Example 10: A bank in Taiwan has customers that are residing in Taiwan but hold German citizenship. The bank is active only in Taiwan; its activities are not directed at the EU market. The bank's processing of the personal data of its German customers is not subject to the GDPR.”

“Example 8: A start-up established in the USA, without any business presence or establishment in the EU, provides a city-mapping application for tourists. The application processes personal data concerning the location of customers using the app (the data subjects) once they start using the application in the city they visit, in order to offer targeted advertisement for places to visits, restaurant, bars and hotels. The application is available for tourists while they visit New York, San Francisco, Toronto, London, Paris and Rome. The US start-up, via its city mapping application, is offering services to individuals in the Union (specifically in London, Paris and Rome). The processing of the EU-located data subjects’ personal data in connection with the offering of the service falls within the scope of the GDPR as per Article 3(2).”

Territoriality of GDPR - Summary

Some actions that could make you subject to the GDPR

- Having an EU country website (www.lab.de)
- Having EU phone number or address
- Translating your website into EU languages
- Accepting EU currency or posting EU currency prices for your services
- Marketing campaign activities targeted to EU patients or businesses
- Processing data in the EU
- EU contract relationships
GDPR Basics 1

• Personal Data: Much broader than PHI under HIPAA:
  Article 4(1): Any information relating to an identified or identifiable natural person (‘data subject’); 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

• Article 9(1): Higher protection for special categories of data (sensitive data):
  – racial or ethnic origin
  – political opinions, religious or philosophical beliefs, or trade union membership
  – genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation
GDPR Basics 2

• Data Controller: Analogous to a covered entity under HIPAA - alone or jointly with others, *determines the purposes and means of the processing of personal data*. Article 4(7) The controller is principally responsible for many GDPR compliance activities we will discuss shortly.

• Data Processor: Analogous to a business associate under HIPAA-*processes personal data on behalf of the controller*. Article 4(8)

• Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Article 4(2)

- Data Controllers must enter into a written agreement with Data Processors in compliance with the GDPR: analogous to a BAA but much more complex
There must be a lawful basis for a controller to process personal data
Article 6(1):
• Consent – freely given, specific, informed and unambiguous by clear action Article 4(11)
• Necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
• Necessary for compliance with a legal obligation to which the controller is subject
• Necessary in order to protect the vital interests of the data subject or of another natural person
• Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
• Necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child – balancing test – not for special categories of personal information
There must be a valid basis to transfer personal data from the EU to a country that does not provide adequate assurances of privacy, and the U.S. is one of those countries

- Signing Standard Contract Clauses Article 46
- Privacy Shield Self Certification Article 46 [https://www.privacyshield.gov/welcome](https://www.privacyshield.gov/welcome)
- Binding Corporate Rules: for transfers between parts of a single organization Article 47
- Derogations: narrow exceptions such as consent, necessary for contract performance, public interest Article 49
Processors and controllers must appoint a Data Protection Officer if the core activities of the processor or controller consist of processing on a large scale of special categories of data (including health data) Article 37(1)
- The DPO must be involved in all issues relating to the protection of personal data Article 38.1
- The DPO must be provided with necessary resources to perform duties and maintain expert knowledge Article 38.2
- The DPO must be reachable by data subjects Article 38.4
- The DPO must be independent, report to the highest management level and not be fired or penalized for exercising their duties Article 38.3
GDPR establishes a set of rights for data subjects – a revolution that is now spreading into U.S. law

• **Right of Access**
  – Controllers are required to provide data subjects upon request:
    • Confirmation whether the controller processes their personal data
    • a copy of their processed personal data – first copy is free – in common electronic form
    • The purpose of processing
    • Categories of data processed
    • Third party recipients of their personal data and the safeguards in place to protect that data
    • Third party sources of their personal data
    • How long personal data would be stored
    • Existence of rights to rectification, erasure, restriction of and objection to processing, and to complain to a supervisory authority
GDPR Basics 7

GDPR establishes a set of rights for data subjects – a revolution that is now spreading into U.S. law

• **Right of Rectification**: Article 16
  - Data subject can obtain from the controller without undue delay the rectification of inaccurate personal data
  - Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed
GDPR establishes a set of rights for data subjects – a revolution that is now spreading into U.S. law

- **Right to Erasure**: Article 17(1)
  - Data subject shall have the right to obtain from the controller the erasure of personal data without undue delay and the controller shall have the obligation to erase personal data without due delay where:
    - The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed
    - The data subject withdraws consent on which the processing is based and there is no other legal ground for the processing
    - The data subject objects and the controller cannot demonstrate compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims
    - The personal data has been unlawfully processed
    - The personal data has to be erased for compliance with EU or member state law to which the controller is subject
GDPR establishes a set of rights for data subjects – a revolution that is now spreading into U.S. law

- **Right to Data Portability**: Article 20
  - The data subject has the right to receive their personal data which he or she has provided to a controller in a structured and commonly used and machine-readable format and have the right to transmit that data to another controller where:
    - Processing is based on consent or a contract and the processing is carried out by automated means
    - The data subject has the right to have personal data transmitted directly from one controller to another where technically feasible
California Consumer Privacy Act https://oag.ca.gov/privacy/ccpa

• Enacted, effective January 1, 2020
• Broad rights for consumers regarding their personal information
  – Right to know what information a business has collected about them, from here, what it is being used for, whether it is being disclosed or sold and to whom
  – Right to opt out of allowing business to sell their personal information
  – Right to have their information deleted, with some exceptions
  – Right to receive the same service and pricing from a business, even if they exercise their rights under the Act, except for a pricing difference that is reasonably related to the value provided to the consumer by the consumer’s data

• Personal information is information that can be associated with a particular consumer or household
• There is a HIPAA-based exemption, but requires that all personal information be treated like PHI
• Applies to business outside California with annual gross revenues greater than $25 million or that receive personal information of 50,000 or more California residents, households or devices annually, or derive 50% or more of their annual revenues from selling California residents’ personal information.
• A business is exempt if every aspect of commercial conduct takes place outside of California – including that the information was collected while the consumer was outside California.
GDPR Approach Is Coming Closer to Home

- Washington Privacy Act—considering a privacy law modeled on the GDPR
- Texas, Hawaii, Massachusetts, New Mexico, Rhode Island, Maryland

More is likely to come, including growing pressure for a federal privacy law
More U.S. Trends Following the GDPR

Risk Management

- **Pseudonymization**
- **Data Protection Impact Assessment required under the GDPR**
  - GDPR requires controllers to assess the impact of proposed processing operations on the protection of personal data Article 35
  - Required for U.S. federal government operations under federal law since 2002: https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments
- **Privacy by Design Article 25**
  - Framework for consideration of privacy issues at the time of the design of a system
  - Proactive
What to do

• Compliance and Privacy Competency and Responsibility
  – Privacy official – DPO
  – Committee
  – Tone at the top
  – Responsibilities
  – Structure
  – Communications
  – Monitoring

• Determine if the GDPR applies
  – Know what can result in GDPR application
  – Plan in advance
  – Intentional decision not inadvertent
What to do

• Address Internal Processes
  – Privacy by Design
  – DPIA process
  – Map flow of PI
  – Address Employee information issues

• Address External Processes
  – Patient consents
  – Flow of information
  – Vendor management
  – Data subject rights

• Manage Risk
  – Check your insurance
  – Monitor
  – Audit
  – Review, Revise
Final Privacy Considerations

• Integrate Privacy into Your Compliance Program
• Make it a top concern
• Get your Board involved
• Monitor Privacy regulations and interpretations
• Be prepared to evolve your privacy compliance
Thank you for your time.

Marty Barrack, MBA, FIP, CIPP/US, CIPP/E, CIPM
SVP, General Counsel and Chief Compliance Officer
XIFIN, Inc.
mbarrack@xifin.com