GDPR and Health Care

Deven McGraw,
Chief Regulatory Officer, Ciitizen

Colin J. Zick,
Partner, Co-Chair, Healthcare Practice and Chair, Privacy & Data Security Practice, Foley Hoag

Brian Annulis,
Senior Managing Director, Ankura

December 5, 2019

Bloomberg Law®

Notes For Participating in Today's Webinar:

- Today's webinar has **2 options** for audio:
  - **Dial In**: Call in to the toll-free conference line using your pin.
  - **Stream on Computer**: Listen using your computer speakers or headphones. If choosing this option, please ensure the volume on your computer is turned up.
- **Questions will not be asked over the phone**. Please submit substantive questions via the "Q&A" window and technical support questions via the "Tech Support" window on the right.
- To access the PowerPoints or other files associated with this webinar, please click on the resources button for listed under the webinar title in your Upcoming Webinars or Recent Registrations on your dashboard.
- If at any time you experience any issues with viewing or hearing the presentation, please press F5 to refresh your screen.

Bloomberg Law®

Receiving Credit For Today's Presentation:

- If you would like to receive credit for attending today's presentation, you will need to respond to the presence check codes popping up on your screen throughout the webinar.
- Please fill out the webinar evaluation survey as well as confirm your certificate information at the end of the webinar.
- For any additional questions, please email credits@bna.com

Bloomberg Law®

THANK YOU TO TODAY'S SPONSOR:

Ankura Consulting Group is a business advisory and expert services firm. Its deep understanding of the opportunities and challenges clients face enables its team to provide impactful, senior-level counsel. As an independent firm built on five key principles – Integrity, Quality, Diversity, Collaboration and Longevity – Ankura's relationships extend beyond one engagement or issue. The firm empowers its industry experts to provide a high-touch, unique approach for its clients in critical times. Ankura's offering includes a wide range of expert witness, turnaround and restructuring, corporate investigation, disputes/litigation support, forensic accounting, geopolitical risk assessment, transaction advisory, valuation, visual communications and business advisory services.

Bloomberg Law®

Does GDPR Apply to me, in the US, in the Healthcare Sector?

Bloomberg Law

- Who is a **Data Subject**?
  - A data subject is a natural person – that is, a human being and not a company – who is a resident of the European Union.

- Is my company a **Data Controller**?
  - A data controller is a person or entity that determines the purposes and means of the processing of personal data.

- Is my company a **Data Processor**?
  - A data processor is a person or entity that processes data under the direction of a controller.

GDPR and HIPAA

The Rights of Data Subjects under GDPR

Bloomberg Law

- **A data subject has a variety of rights under the GDPR, some of which look like rights under HIPAA:**
  - The right to **correct** Personal Data that is incorrect or incomplete.
  - The right to **ask** what Personal Data has.
  - The right to request that that the data controller **limit** processing of data for particular purposes.
  - Data subjects should be **informed** of their rights by your privacy policy.

- **And some don't look like HIPAA rights:**
  - The right to request that **delete** Personal Data, or only process data for particular purposes.
  - The right to request that **stop** processing Personal Data.
  - The right to **withdraw** consent to use data at any time.

Lawful Data Collection under GDPR

Bloomberg Law

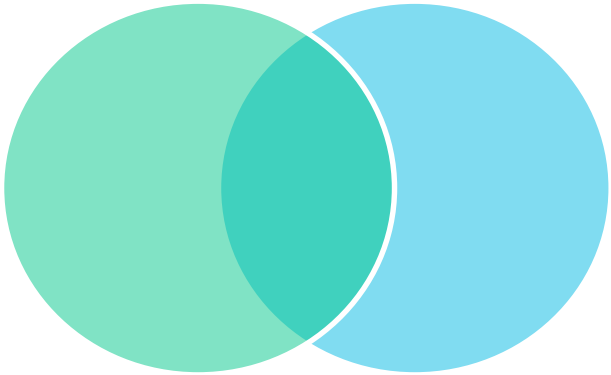
- **Before seeking to collect Personal Data, think about the following questions:**
  - Do I **need** to collect Personal Data to accomplish what I'm trying to accomplish?
  - Do I know the **geographic source** of the Personal Data (or, at least, whether it is from an EU resident)?
  - Do the data subjects know **what** data I am collecting and **why**?
    - Have I directed any relevant data subjects to your privacy policy?
  - If I am communicating for **marketing purposes**, has the recipient explicitly **opted-in** to receiving marketing communications?

Bloomberg Law

General Data Protection Regulation (GDPR)

Significant overlap with CCPA

- Right to disclosure and access
- Right to data deletion
- Type of information regulated (identifiable to individual)
- Definition of “personal information”
- Privacy notice requirement
- Security measures requirement
- Extraterritoriality



But significant differences

- Scope and territorial reach (GDPR is broader)
- Right to opt-out (GDPR doesn’t provide one)
- Children’s data (GDPR is more protective)
- Right to rectification (CCPA doesn’t provide one)
- Private right of action (GDPR is broader)

Research Under HIPAA

- **HIPAA General Proposition**
  - Without an individual's Authorization, a Covered Entity (or Business Associate) may not use or disclose PHI except as permitted or required by the Privacy Rule

- **Research**
  - Research is defined by the Privacy Rule as a "systemic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." (45 CFR 164.501)
    - Key point—goal must be generalizable knowledge, otherwise likely a HCO specific to the CE
  - Research is a permitted use and disclosure of PHI under the Privacy Rule (45 CFR 164.512(i))
  - The use and disclosure of PHI for Research should be stated in the Covered Entity's Notice of Privacy Practices (45 CFR 164.520)

Research Under HIPAA - How?

- With an Individual's written Authorization (45 CFR 164.508)
- Waiver of Written Authorization by IRB/Privacy Board (45 CFR 164.512(i)(1)(i))
- Limited Data Sets of PHI (45 CFR 164.514(e))
- De-identified Health Information (45 CFR 164.514(a))

Research Under GDPR

GDPR requires Controllers and Processors to have a lawful basis for processing any Personal Data about an individual in the EU, including Sensitive Personal Data (Art. 6 & 9)

Research Under GDPR - Consent

- GDPR generally requires a Controller to either obtain a person's consent to process Personal Data or have another lawful basis for processing the Personal Data

- Consent under GDPR (Art. 7)
  - Freely given, specific, informed, unambiguous (and explicit)

- Like HIPAA, Consent for Use and Disclosure of Personal Data for Research under GDPR is not the same as Informed Consent for Research

- Like HIPAA, GDPR allows for the processing of Personal Data for Research (Art. 89).
  - Data minimization is encouraged
  - Data minimization promotes the use of Anonymized and Pseudonymized data to the extent possible

Research Under GDPR—How?

- With an Individual's Consent
- Pursuant to another Lawful Basis, including Scientific Research
  - Anonymized Data
  - Pseudonymized Data
  - Likely requires Data Processing Agreements, Materials Transfer Agreements, Data Use Agreements between Personal Data Controllers and Processors

Commercialization of Research Data

Bloomberg Law

HIPAA Constraints

- Post HITECH, the Privacy Rule specifically prohibits the Sale of PHI without Individual Authorization (45 CFR 164.508(a)(4))
- Sale of PHI does not include disclosure of PHI for Research, but remuneration is limited to cost-based fees (45 CFR 164.502(a)(5)(ii))
- A LDS of PHI is still PHI (hence limitations on Sale of PHI still apply—i.e., cost based fees)
- De-identified health information

GDPR Constraints

- Consent freely given, specific, informed, unambiguous, and explicit (for Sensitive Personal Data, including health, genetic, and biometric information)
- Pseudonymised Data is still Personal Data
  - Data Processing Agreement, Materials Transfer Agreement, Data Use Agreement
- Anonymized Data

Flipping the paradigm: user-controlled data

Bloomberg Law

- New companies emerging that aim to give users the ability to share and even monetize their data.
  - Examples: digi.me, hu-manity.co, LunaDNA

- Example of health data research initiatives driven by patient data donation: NIH All of Us Research Program, Ciitizen-Cholangiocarcinoma Foundation registry partnership

- Rights to data access in HIPAA and GDPR open opportunities for data – and databases - controlled by users or advocacy groups.

- HIPAA and GDPR access rights are comparable – in US, HHS OCR getting more assertive in enforcing HIPAA rights.

Comparison of Individual Rights Provisions

Bloomberg Law

	Right to be Informed	Right to restriction of processing	Right of access/copy	Right of erasure	Right to rectification	Data portability
GDPR	Requires detailed disclosures on data practices, including info collected, purposes for processing, categories of recipients, etc.	Right to get controller to restrict processing under certain circumstances (where accuracy of data is contested; processing is unlawful, for example); required to inform downstream recipients unless this is impossible or involves disproportionate efforts	Right to know what information controller has, right to obtain copies (within 30 days; free unless request is excessive)	Aka the "right to be forgotten;" applies if no longer basis for lawful processing or other reasons; must use reasonable efforts to communicate to downstream recipients	Right to obtain rectification of inaccurate personal data (includes right to have incomplete personal data completed through supplementary statement)	Right to receive personal data in a structured, commonly used and machine readable format and the right to transmit that data to another controller without hindrance, where processing is based on consent and processing is carried out by automated means
HIPAA	Notice of Privacy Practices must cover only what entity has right to use/disclose, individual rights (like a HIPAA explanation)	Right to request restriction (no requirement to honor except w/r/t disclosure to health plans for services paid for in full out of pocket)	Right to copy (within 30 days but reasonable, cost-based fee can be charged for labor associated with making the copies)	None	Right of amendment is right to "request" amendment; however must honor individual's right to submit her version (which must be appended to data)	Right to digital copy of information maintained digitally; right to copy in form and format requested if reproducible in that form/format; right to have copy directly to designated third party

Benefits & Pitfalls

- **Benefits:**
  - Data initiatives operate with patient/consumer consent, opportunity to create more trusted platforms
  - Patients/patient groups with data have stronger voice in choosing research questions, setting research priorities
  - May bypass some logistical hurdles to getting multi-site research done
- **Challenges:**
  - Achieving critical mass
  - Enforcement of data rights provisions
  - Same challenges faced by companies in getting meaningful, informed consent of data subjects
  - In US, consumer-facing entities not subject to HIPAA – regulated only by FTC and adherence to privacy commitments (would be likely be covered as data controllers under GDPR)

How Can You Ensure GDPR Compliance/ Reduce Enforcement Risk?

Bloomberg Law

- You don’t need to be a GDPR expert, but everyone can help to spot issues when they arise.

- A few issues you can help spot:
  - When enters a contract with an online service provider, does that contract address GDPR?
  - When you communicate with potential customers and business partners, do you know whether you are receiving Personal Data about EU residents?
  - When you send marketing communications, has opt-in consent to marketing communications been obtained?
  - When EU residents seek to exercise a GDPR right, is that request forwarded to the relevant person?

- When you spot an issue, seek additional guidance from your data protection officer.

What We Have Learned About GDPR Risks Since May 2018

Bloomberg Law

- **Data breaches are actively being reported to supervisory authorities.**
  - In the first 18 months of GPDR, tens of thousands of breaches were reported to EU supervisory authorities.
  - Fines have generally been low
- **Supervisory authorities are actively enforcing the GDPR, but are prioritizing certain kinds of companies for enforcement.**
  - Major internet companies.
  - Large outside-of-EU companies (particularly U.S. companies).
  - Companies that process or control health data.
- **Companies are becoming more aware of GDPR.**
  - Many major online service providers make GDPR a regular part of contracting with business partners.

Personal Data Risks: Anonymization and Pseudonymization Under GDPR

Bloomberg Law

- Recital 26 of the GDPR defines anonymized data as “data rendered anonymous in such a way that the data subject is not or no longer identifiable.”

- Article 4(5) of GDPR defines “pseudonymization” as the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, with technical and organizational measures to ensure that they are not attributed to an identified or identifiable natural person.

- GDPR defines pseudonymization as an act of processing, and not as a category of personal data.

    - It is therefore inadvisable to use the definition of pseudonymization to determine whether data are personal data.

Data Privacy Program - Developing a Risk Strategy

Bloomberg Law

- **Starts with Data Inventory and mapping Data flows**
  - What Data to you use, disclose, maintain, process or control?
  - Where does your Data reside? Flow?

- **What is the organization's Data Privacy Philosophy/Framework?**
  - How/why do you use/intend to use and disclose Data?
  - Interested in building a Data warehouse for Research or other purposes?

Data Privacy Program—Implementing a Risk Mitigation Strategy

Bloomberg Law

- Has your organization completed a Data Privacy/Security Risk Assessment?
- Do you have a CPO? CISO? DPO?
- Do you have an incident response plan in place for identifying and addressing Breaches?
- Do you have the requisite contracts in place with third-parties that access, maintain, use or disclose your Data?
- In addition to legal considerations, what other issues factor into/should factor into your Data Privacy Program and risk mitigation strategy?