COPPERSMITH
BROCKELMAN
LAWYERS

The General Data Protection Regulation (GDPR) and its Impact on US Healthcare Entities

HCCA – Nashville Regional Compliance Conference
November 16, 2018

Kristen B. Rosati
Coppersmith Brockelman PLC
krosati@cblawyers.com
602-381-5464

Questions We'll Explore Today

- When does the GDPR apply to healthcare organizations in the US?
- How will the GDPR affect consent for clinical care and research activities?
- How will the GDPR affect the maintenance, use and disclosure of personal data in electronic health records and other clinical information systems?
- What else do we have to worry about?

What is the jurisdictional reach?

- New EU data protection law, effective May 25, 2018
- Applies to organizations "established" within the European Economic Area (EEA): the EU + 3 (or + 4 after Brexit)
- Applies to organizations outside the EEA that:
  - Offer goods or services to data subjects within the EEA
  - Monitor the behavior of data subjects within the EEA

COPPERSMITH BROCKELMAN LAWYERS

3

What is the jurisdictional reach?

- Offering goods or services to data subjects within the EEA (whether or not payment received)
  - Merely treating patients that are from the EEA countries will not trigger the GDPR
  - Having a website that is accessed by EEA data subjects will not trigger the GDPR, but directing the website to EEA data subjects (through language translation or offering services in EU currency) will trigger
  - Telemedicine arrangements
  - Consulting or referral arrangements
  - Clinical trial recruitment of EEA data subjects

COPPERSMITH BROCKELMAN LAWYERS

4

What is the jurisdictional reach?

- Monitoring the behavior of data subjects in the EEA
  - Tracking on the internet
  - Collection of data from mobile devices (even if data subject only temporarily located in the EEA)

COPPERSMITH BROCKELMAN LAWYERS

Why care about the GDPR?

- Extensive individual rights with private right of action
- FTC may enforce GDPR within the US
- *BIG PENALTIES – UP TO 20 MILLION EUROS or 4% annual "turnover" (gross revenue)*

COPPERSMITH BROCKELMAN LAWYERS

What if the GDPR applies?

- Data "controller" (determines the purposes and the means of processing personal data) vs. data "processor" (processes personal data on behalf of a controller)
- Extensive data controller responsibilities
  - Providing notices to data subjects
  - Implementing data subject rights
  - Notice of data breaches to data protection authorities and data subjects within 72 hours
  - Implementing technical safeguards
  - Enacting policies
  - Doing data protection "impact assessments" if high risk to individuals
  - Designating a data protection officer
  - Appointing EEA representative
  - Maintaining records of data processing

COPPERSMITH BROCKELMAN LAWYERS

7

What is "personal data"?

- Any data that directly or indirectly identifies a living individual (not just patients)
  - Name, identification number, location data, online identifier, factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity
- More sensitive data have special protection
  - Genetic data, biometric data for the purpose of creating unique identification, data concerning health, data regarding race, religion, politics, sex
- Treatment of de-identified data
  - Pseudonymised (coded) still personal data – no de-identification "safe harbor"
  - Anonymous data (not linked)-- not personal data

COPPERSMITH BROCKELMAN LAWYERS

8

What are data subject rights?

- Right to erasure (right to be forgotten) (with some exceptions)
- Broader access rights than HIPAA and CLIA
- Notice of data breaches
  - Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data
  - If likely to result in a high risk to the rights and freedoms of natural persons, controller must report to the data subject without undue delay

COPPERSMITH BROCKELMAN LAWYERS

9

When is consent required?

GDPR requires a legal basis for "processing" data

- Consent;
- Necessary for compliance with a legal obligation of "controller";
- Necessary for purposes of the "legitimate interests" of the controller; or
- Other provisions not generally relevant in the healthcare setting

COPPERSMITH BROCKELMAN LAWYERS

10

When is consent required?

- GDPR requires additional legal basis for processing special categories of sensitive data
  - Explicit consent;
  - Necessary for preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment;
  - Necessary for public health;
  - Necessary for scientific research; or
  - Other provisions not generally relevant in the healthcare setting

COPPERSMITH BROCKELMAN LAWYERS

11

If consent is required…

- Guidance from the "Working Party" requires consent to be:
  - Freely given
  - Specific
  - Informed
  - An unambiguous indication by a statement or a clear affirmative action
- Data subjects have the right to withdraw consent

COPPERSMITH BROCKELMAN LAWYERS

12

What if the GDPR doesn't apply to you directly?

- Requirements for transfer of personal data from the EEA to the US may apply to the sender:
  - Consent (and advising data subjects of the risks of transfer to the US);
  - Contract that contains model contractual clauses approved by the European Commission (which impose some GDPR requirements on receiving entity);
    - Specific requirements for contracts with data processors
  - To US for-profit entities that have been certified under the EU-US "Privacy Shield"; or
  - Pursuant to codes of conduct by associations

COPPERSMITH BROCKELMAN LAWYERS

What if the GDPR doesn't apply to you directly?

- Recipient requirements to receive personal data from the US:
  - Recipient may require specific consent to process data within the EEA
  - Recipient may require distribution of notice regarding data processing activities

COPPERSMITH BROCKELMAN LAWYERS

What are next steps for US healthcare organizations?

- Do you do any business with organizations in the EEA?
  - Telemedicine arrangements?
  - Referral or second opinion arrangements?
  - Any branding arrangements?
  - Vendors located in the EEA?
- Do you do any specific outreach to patients, physicians or others in the EEA? Advertising or public relations activities?
- Is your website translated into EEA member state languages? Or do you quote prices in EEA currencies?
- Do you track visitors to your website?

COPPERSMITH BROCKELMAN LAWYERS

What are next steps for US healthcare organizations?

- Do you participate in any multi-site studies with other sites in the EEA?
- Do you have any data coming into your organization from the EEA? Have you done a data flow map?
- If you are subject to the GDPR, develop a project plan!

COPPERSMITH BROCKELMAN LAWYERS

COPPERSMITH
BROCKELMAN
LAWYERS

Kristen Rosati
Coppersmith Brockelman PLC
krosati@cblawyers.com
602-381-5464

This educational presentation is not legal advice.
Please consult your legal counsel for advice on your particular circumstances.