WHAT HEALTHCARE ORGANIZATIONS NEED TO KNOW ABOUT THE EUROPEAN UNION’S GENERAL DATA PROTECTION REGULATION (GDPR)
OVERVIEW

• New EU General Data Protection Regulation (GDPR) published in EU Official Journal on May 4, 2016 and will apply across the EU from **May 25, 2018**.

• Regulation will replace the existing Data Protection Directive and be directly applicable to all processing of personal data in the EU / collected from EU data subjects.

• In theory, a goal of the Regulation is to achieve greater harmonization of requirements across EU. However, in many contexts, potential for variation exists.

• Regulation includes significant **escalation in potential penalties** as compared to current law. Violations can result in fines of up to 4% of an entity’s global revenues.
TERRITORIAL SCOPE OF THE GDPR

• GDPR 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 or not the processing takes place in the Union or not.

• GDPR 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:
  • The offering of goods or services, irrespective of whether payment of the data subject is required, to such data subject in the Union, or
  • The monitoring of their behavior as far as their behavior takes place within the Union.

• GDPR applies to the processing of personal data by a controller not established in the Union, but in place where Member State law applies by virtue of public international law.
GDPR

• The Directives
• Chapter I – General Provisions
• Chapter II – Principles
• Chapter III – Rights of the Data Subject
• Chapter IV – Controller and Processor
• Chapter V – Transfer of Personal Data to Third Countries or International Organizations
• Chapter VI – Independent Supervisory Authorities
• Chapter VII – Cooperation and Consistency
• Chapter VIII – Remedies, Liability and Penalties
PROTECTION OF PERSONAL DATA AS A FUNDAMENTAL RIGHT

• The protection of natural persons in relation to the processing of personal data is a fundamental right.
  • Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter) and
  • Article 16(1) of the Treaty on the Functioning of The European Union (TFEU)

• Directive 95/46/EC of the European Parliament and of the Council seeks to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

• GDPR respects all fundamental rights and observes the freedoms and principles enshrined in the Treaties, in particular with respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial and cultural, religious and linguistic diversity.
DEFINITION OF PERSONAL DATA

• “Personal Data” means any information relating to an identified or an 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 of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
PRACTICE NOTE: COMPARISON OF “PERSONAL DATA” UNDER GDPR TO “PHI” UNDER HIPAA

• Personal Data is not just health data

• Personal Data applies all health data (PHI is only health data created by Covered Entities)

• HIPAA allows for two methods of de-identification of data – the Safe Harbor method and statistical certification. De-identified data is no longer PHI. European DPAs are typically skeptical of the HIPAA Safe Harbor approach to de-identification.

• As a matter of terminology, Europeans prefer the term “anonymization” to “de-identification.” Some DPAs will assert that anonymization is a higher standard.
OTHER DEFINITIONS

• “Controller” means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

• “Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

• “Processing” means any operation or set of operations which is performed on Personal Data...
PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

- Personal Data shall be:
  - Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness & transparency);
  - Collected for specified, explicit and legitimate purposes… (“purpose limitation”);
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimization”);
  - Accurate and, where necessary, kept up to data… (“accuracy”)
  - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed… (“storage limitation”);
  - Processed in a manner that ensures appropriate security of the personal data… (“integrity and confidentiality”)

9
LEGAL BASES FOR PROCESSING PERSONAL DATA

Processing shall be lawful only if and to the extent that at least one of the following applies:

• Data subject consents,

• Processing is necessary:
  • For the performance or negotiation of a contract with the data subject;
  • To comply with a legal obligation;
  • To protect the vital interests of the data subject or another person when the data subject is incapable of giving consent
  • For the performance of a task carried out in the public interest or the exercise of official authority; and
  • For the purposes of legitimate interests (but subject to fundamental rights and freedoms).
Lawfulness of Processing

- Consent
- Performance of Contract
- Compliance with Legal Obligation
- Public Interest
- Legitimate Interests
- Vital Interests
CONSENT

• **Demonstrate Consent:** Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.

• **Clear and Plain Language:** The request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

• **Right to Withdraw Consent:** The data subject shall have the right to withdraw consent at any time.

• Consent does not provide a valid legal justification for processing where there is an imbalance that makes it unlikely that consent was given freely (e.g., employer-employee situations).

• Where performance of a contract or receipt of a service is made conditional on consent to processing for purposes other than those that are necessary to performance of the contract or providing the service, such consent may not be considered freely given.
HEALTH DATA AND OTHER SPECIAL CATEGORIES OF PERSONAL DATA

• Special Categories where the processing of personal data is prohibited unless one of the specific exceptions apply:
  • Personal data revealing racial or ethnic origin
  • Political opinions
  • Religious or philosophical beliefs
  • Trade-union membership
  • Genetic data or 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
EXCEPTIONS TO PROHIBITION ON PROCESSING OF SENSITIVE DATA

• The processing is necessary for **reasons of substantial public interest**, where such public interest is based in EU or member state laws.

• The processing is **necessary for the purposes of preventive medicine, medical diagnosis, the provision of health care or treatment, or the management of health care systems and services**, where such processing is (i) based on EU or member state laws, or (ii) conducted pursuant to a contract with a health professional subject to an obligation of professional secrecy under EU or member state laws or rules established by national competent bodies.

• The processing is necessary for **reasons of public interest in the area of public health**, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices, where such processing is based on EU or member state laws.

• The processing is **necessary for scientific research purposes**, where such processing is based on EU or member state laws.
Processing of Sensitive Data

- Consent
- Employment Law
- Vital Interests
- Charity / Not-for-Profits
- Public Data
- Legal Claims
- Substantial public Interest
- Medical Purposes
- Public Health
- Scientific Research
PRACTICE NOTE: CONSENT IN HEALTH CARE CONTEXT

• View of European data protection authorities is that consent often does not provide a legal basis for the processing of personal data in the health care context (because consent often cannot be withheld by the data subject without detriment).

• Instead, other legal bases should be relied upon.
DATA SUBJECTS RIGHTS

- **Right to Rectification:** The right to require rectification of Personal Data without undue delay and the right to have incomplete personal data completed;

- **Right to be Forgotten:** The right to erase personal data when processing is no longer necessary; consent is withdrawn, legitimate interests no longer apply, processing is unlawful, or erasure is required by law and the controller must take reasonable steps to inform other controllers if it has made such data public;

- **Right to Restriction:** When there is a dispute as to the accuracy, when an objection to processing has been verified, when processing is unlawful and the data subject objects to erasure, or when the data is no longer required by the controller but the data subject requires it for the establishment exercise or defense of a legal claim; and

- **Data Portability:** The right to require that the data provided by the data subjects for processing with their consent or under contract to be provided in a commonly used and machine-readable form and transmitted to another controller.
DATA SECURITY REQUIREMENTS

• **Security Measures:** Controls and processors must each apply appropriate technical and organizational security measures to guarantee an adequate level of protection for personal data.

• **Pseudonymization:** Where appropriate, security measures must include pseudonymization and encryption, the ability to restore personal data in a timely manner, and regular testing and assessment.
BREACH NOTIFICATION

• **72 hours reporting by Controllers:** Controllers must report personal data breaches to the relevant supervisory authority without undue delay (when feasible, within 72 hours of becoming aware of the breach), unless the breach is unlikely to put the data subjects’ rights and freedoms at risk.

• **Notify data subjects:** Controllers must notify affected data subjects of personal data breaches if the breaches pose significant risks to the data subjects’ rights and freedoms.

• **Reporting by Processors:** Processors must report personal data breaches to the controllers without undue delay in all cases.
DATA PROTECTION OFFICER

• The GDPR requires that an organization appoint a DPO if processing sensitive personal data on a large scale or engaged in regular and systematic monitoring of data subjects on a large scale.

• A single DPO may be appointed for a group of companies, provided the DPO is readily accessible from each of the group’s establishments.

• Where a DPO is required, this person must report directly to the highest management level.

• DPO must be in a position to perform tasks in an independent manner, should not receive any instructions regarding the exercise of his/her tasks, and may not be dismissed or penalized for performing those tasks.
• Data protection must be considered (and such considerations documented) in the design of all new processes and technologies for the processing of personal data.

• Written DPIAs required whenever processing involves high risks to data subjects, such as processing of sensitive data and whenever automated processing results in decisions having legal effect. DPIA may evaluate an entire category of processing operations if they are sufficiently similar.

• DPIA must identify specific risks and describe privacy and security measures implemented to mitigate them.

• Mandatory consultation with data protection authority where processing poses high level of risk to data subjects that cannot be adequately mitigated.
• **Remedies:** Data subjects have the following rights against controllers and processors:
  • The right to lodge complaints
  • The right to appeal decisions before national courts
  • The right to initiate judicial proceedings before the national courts of establishment of the controller or processor or of the data subject’s residence

• **Sanctions:** Administrative fines
  • Fines can be up to 20 million Euros or in the case of undertakings, 4 percent of annual worldwide turnover whichever is higher
  • Fines must be determined on the basis of criteria listed in the GDPR and are subject to judicial review and due process
  • EU Member States can impose additional penalties, including criminal sanctions.
HYPOTHETICALS – TERRITORIAL SCOPE

• A German citizen comes to the United States to receive special surgery.
  • Generally, NOT COVERED BY GDPR because the data subject is not in the Union.
  • But, if hospital were to specifically target European residents in order to promote international medical travel to the US, then GDPR could apply.

• US citizen receives medical care in Europe.
  • GDPR would apply to a US citizen in Europe.

• A pharmaceutical company conducts a research study in Greece
  • GDPR would apply because the data subjects are in the Union.
HYPOTHETICALS – TERRITORIAL SCOPE

- A hospital in the US offers telemedicine services to patients in Sweden (e.g., reading medical scans to provide a second opinion).
  - GDPR would apply because the data subjects are in the Union.

- U.S. health system offers consulting and training to EU-based health care systems and HCPs.
  - GDPR would apply to associated processing of personal data.

- U.S. academic medical center engages in a partnership with EU-based health care institutions.
  - GDPR would apply to processing of personal data that occurs in the context of that partnership and that involves data of EU individuals or processing of data in EU.
HYPOTHETICALS REGARDING WEBSITES

• A US hospital has a website in the US that can be accessed in Europe
  • Not enough to trigger GDPR

• A health technology vendor based in the US that provides software solutions for physicians has a website where online orders can be placed in foreign currencies and the website uses the language of the country of origin
  • This activity would trigger GDPR compliance requirements

• A small medical device company based in the US has patient testimonials from patients from various European countries.
  • This website would trigger GDPR compliance requirements.
QUESTIONS & ANSWERS