Data Privacy Laws: Their Impact on US Healthcare and What You Need to Know

Rebecca L. Rakoski, Esq.
XPAN Law Group, LLC

The Evolution of Data Privacy

GDPR Scope (Art. 1):

Applies to the **“processing”** and free movement of “personal data” of a “natural person” within the EU

GDPR Scope (Art. 1):

Applies to applies to the “processing” and free movement of **“personal data”** of a “natural person” within the EU

GDPR Scope (Art. 1):

Applies to applies to the “processing” and free movement of “personal data” of a “**natural person**” within the EU

Key Roles:

- Controllers
- Joint Controllers
- Processors
- Sub-processors

Comparing the GDPR & HIPAA

	GDPR	HIPAA
Consent	Permits the use of health-related personal data with explicit consent from the subject, unless reliance on consent is prohibited by EU or member state law.	Permits the use or disclosure of PHI pursuant to an individual's authorization, which must include a number of required elements.
Carrying out employment, social security or social protection obligations	Permits the processing of sensitive personal information for the carrying out of obligations under employment, social security or social protection law, or a collective agreement.	Permits use or disclosure of PHI as authorized by laws relating to workers' compensation but generally prohibits use of PHI for employment purposes.

Comparing the GDPR & HIPAA

	GDPR	HIPAA
Protecting vital interests when the subject is incapable of providing consent	Permits processing sensitive personal information, such as health-related personal data, when necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent.	Permits disclosure to an individual's personal representative who would presumably be in a position to protect the individual's vital interests where the individual is incapable of making certain decisions.
Not-for-profit entities	Permits processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent.	Does not have a similar use or disclosure provision.

Comparing the GDPR & HIPAA

	GDPR	HIPAA
Information made public by the subject	Allows entities to process data manifestly made public by the data subject.	Diverges from GDPR and provides the opposite — such a use or disclosure by the data subject has no effect on the protections afforded by HIPAA.
Judicial proceedings	Permits processing that is necessary for the establishment, exercise or defense of legal claims or where courts are acting in their judicial capacity.	Permits disclosure of PHI in the course of a judicial or administrative proceeding.

Source: *IAPP*, https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/

Comparing the GDPR & HIPAA

	GDPR	HIPAA
Public interest & required by law	Permits processing sensitive personal information necessary for reasons of substantial public interest on the basis of EU or member state law that is proportionate to the aim pursued and which contains appropriate safeguarding measures.	Provides for the use or disclosure of PHI as required by law. This means that a mandate contained in law that compels an entity to use or disclose PHI and that such use or disclosures is enforceable in a court of law.
Research	Permits processing sensitive personal information for scientific and historical research purposes or statistical purposes.	Provides that PHI may be used or disclosed for research purposes.

Source: *IAPP*, https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/

Comparing the GDPR & HIPAA

	GDPR	HIPAA
Medical treatment	Provides for the processing of sensitive personal information when necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or member state law or a contract with a health professional.	Permits the use or disclosure of PHI for treatment purposes which includes provision, coordination or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
Public health	Permits processing of sensitive personal information that is necessary for public interest reasons in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.	Permits use or disclosure of PHI to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations or interventions.


ONE DOES NOT SIMPLY
IGNORE GDPR COMPLIANCE


QUEBEC
ONTARIO
NB
PE
NOVA SCOTIA
WASHINGTON
MONTANA
NORTH DAKOTA
Ottawa
MAINE
VT
NH
OREGON
IDAHO
NEW YORK
MA
CT
WYOM
PENN
Philadelphia
MD
DE
San Francisco
NEVADA
UTAH
CALIFORNIA
Las Vegas
Los Angeles
NORTH CAROLINA
SOUTH CAROLINA
ARIZONA
NEW MEXICO
MISSISSIPPI
Dallas
GEORGIA
TEXAS
LOUISIANA
CALIFORNIA
• California Consumer Privacy Act of 2018

Key Takeaways:

1. GDPR and HIPAA do not replace each other but must be complied with concurrently

1. Being HIPAA compliant does not mean you are CCPA compliant.

1. GDPR applies to ALL Personal Data, and not just Medical Information

1. GDPR and HIPAA both require formal agreements to be in place to share information

For further information or questions, please contact me at: rrakoski@xpanlawgroup.com

---