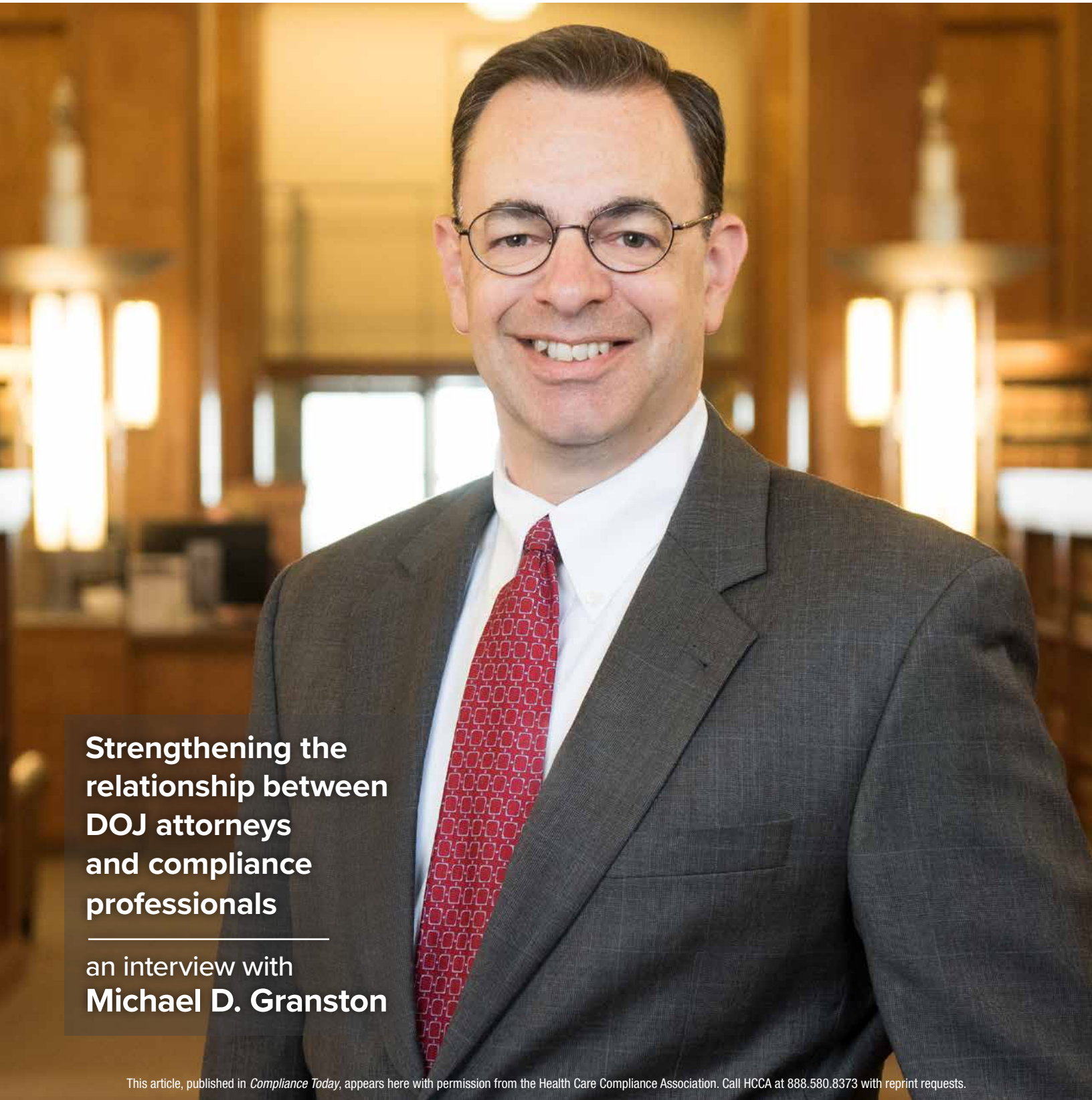
HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

SEPTEMBER 2018



Strengthening the relationship between DOJ attorneys and compliance professionals

an interview with
Michael D. Granston

by Adam H. Greene, JD, MPH and Lyra Correa, JD

Is the sky falling? GDPR implications in the US

» The General Data Protection Regulation (GDPR) applies if you operate in or market to the European Union (EU).
» Website monitoring of users may subject you to GDPR.
» GDPR mostly overlaps with HIPAA, but with key differences.
» De-identified information under HIPAA may still be subject to GDPR.
» For those subject to GDPR, the potential penalties are significant.

Adam H. Greene *(adamgreene@dwt.com) is a Partner in the Washington DC office of Davis Wright Tremaine LLP and co-chair of its Health Information Practice Group.* ***Lyra Correa*** *(lyracorrea@dwt.com) is an Associate in the Washington DC office of Davis Wright Tremaine LLP.*
bit.ly/in-Adam-Greene *bit.ly/in-LyraCorrea*

Pop quiz: An injured Belgian tourist appears at your door for treatment. Do you:

A: Pay to medevac her across the Atlantic and unceremoniously dump her on the shores of Achill, Ireland (the closest spot to the U.S. in the European Union (EU)
B: Handwrite all her medical notes on the back of napkins and burn them at discharge
C: Shutdown the facility for a week while you scramble to come into compliance with the EU's General Data Protection Regulation (GDPR)[1]
D: Treat her like a regular patient and protect her information in accordance with the Health Insurance Portability and Accountability Act (HIPAA)[2]

If you answered A, B, or C, then it's time to take a deep breath and relax. And possibly revisit your Emergency Medical Treatment and Active Labor Act (EMTALA) compliance.

The most reasonable answer is D. Although there are many frantic headlines regarding GDPR, it will likely have limited impact on most US healthcare providers. US healthcare providers should carefully review whether they fall under GDPR, including through marketing efforts and website information collection. If GDPR is applicable, then it is not too late to begin compliance, and HIPAA is a very good place to start.


Greene


Correa

What is the GDPR?

GDPR is a new set of rules drafted by the EU that are designed to provide a stronger set of protections to give individuals in the European Economic Area (EEA) (i.e., the 28 EU countries plus Norway, Iceland, and Liechtenstein) more control over their personal data. GDPR regulates the collection, use, disclosure, and other "processing" of personal data by "controllers" and "processors." A "controller" is an entity that determines the purposes and means of the processing of personal data, while a "processor" is an entity that processes the

personal data on behalf of the controller. The relationship of the controller and processor is analogous to the relationship between a covered entity and a business associate. The processor (business associate) processes data on behalf of a data controller (covered entity) and is required to protect the data the same way that a controller would. Like HIPAA, GDPR also requires controllers and processors to implement technical and organizational measures to prevent breaches of the personal data. GDPR does not refer to "citizens" or "residents," but rather applies to the processing of personal data of any person in the EU (a "data subject"), even if the person is only in the EU temporarily.

Stateside impact?

HIPAA may not apply to entities located outside of the U.S. because neither the HIPAA statute nor the regulations address extraterritoriality, and Congress gave no indication that it intended HIPAA to apply outside of the U.S. Unlike HIPAA, GDPR has direct extraterritorial reach to entities that process the personal data of EU data subjects, regardless of whether the processing takes place within the EU. The good news is that GDPR will not affect a majority of US healthcare providers and only affects healthcare providers that are:

- Physically located in the EU,
- Market to EU data subjects, or
- Monitor data subjects' behavior for activities taking place in the EU.

Marketing to EU data subjects involves more than EU data subjects having mere access to a US healthcare provider's website or general global marketing. However, if a US healthcare provider actively pursues EU data subjects (e.g., by converting to EU currency on the provider's website, offering a website specific to an EU country, marketing in the language of the EU country), then GDPR will apply.

Monitoring the behavior of EU data subjects relates to collecting information about an EU data subject's activities while the data subject is in the EU. For example, as we go from website to website, different websites track information about us, such as what we click on, for purposes of building a profile about us. This is often used to target specific advertisements to us. If a US company collects this information while an individual is using the Internet from the EU, then the US company will become subject to GDPR.

In the scenario above, if the US provider that treated the Belgian patient did not market to the EU to try to attract EU patients and does not continue to provide treatment to the patient after she returns to the EU (e.g., telemedicine), then GDPR is unlikely to apply. However, if the US healthcare provider has a website specifically designed to attract Europeans, or uses website cookies for purposes of creating profiles about the online behavior of patients (or anyone else for that matter) when they are in the EU, then GDPR may become applicable to the US healthcare provider.

In determining whether GDPR is applicable, US healthcare providers should focus on questions such as:

- Do we have offices in the EU?
- Do we operate in the EU, such as by performing clinical research in the EU in partnership with EU institutions?
- Do we advertise in the EU?
- Does our website include features clearly aimed at attracting EU patients (not just international patients generally)?
- Does our website include monitoring of patients or other website visitors

(e.g., tracking website visitors' behavior through website cookies or other means) that may capture behavior of EU data subjects?

Even if not directly subject to GDPR, US healthcare providers and other healthcare entities should also be careful about contractually agreeing to comply with GDPR. For example, certain online service providers may interpret that they are required to pass on GDPR-related contractual provisions to anyone who uses their services.

GDPR vs. HIPAA

For the small portion of US healthcare providers who must comply with GDPR, it is important to grasp the differences between HIPAA and GDPR. The following details some key differences between each law.

HIPAA's "PHI" vs. GDPR's "data concerning health"

Unlike HIPAA, GDPR protects all "personal data," which is defined as any data that can be used to directly or indirectly identify a living person, but HIPAA's protections only apply to protected health information (PHI). GDPR's broad definition of personal data includes "sensitive personal data," such as racial or ethnic origin, political opinions, biometric data, religious or philosophical beliefs, trade union membership, genetic data, data concerning a natural person's sex life or sexual orientation, and data concerning health. GDPR's definition of "data concerning health" is very similar to PHI and is defined as personal data relating to the physical or mental health of an individual, including the provision of healthcare services, which reveal information about a person's health status. PHI is defined under HIPAA as individually identifiable information relating to past, present, or future physical or mental health condition, the provision of healthcare, or payment of healthcare.

Scope of GDPR vs. HIPAA

GDPR applies to all controllers or processors, regardless of the type of personal data they process or handle, and the reason they need to use the data. HIPAA, on the other hand, regulates only HIPAA covered entities and business associates. Covered entities are defined as: (1) health plans, (2) healthcare clearinghouses, and (3) healthcare providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. A business associate is an entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity.

> Under GDPR, individuals have the right "to be forgotten."

Right to erasure

Under GDPR, individuals have the right "to be forgotten." In other words, individuals have the right to have their personal data erased under certain circumstances. HIPAA on the other hand, does not have a right to erasure, and in fact, mandates that entities retain certain compliance-related documentation, which may sometimes include limited PHI, for six years from the date of its creation or the date when it was last in effect, whichever is later. The GDPR recognizes that healthcare

organizations may need to retain personal data for regulatory and legal obligations, but such exceptions to erasure are less clear-cut than under HIPAA.

Data identification vs. anonymization

Under HIPAA, health information that "does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, is not individually identifiable health information." Such de-identified information is no longer subject to the protections of HIPAA. There are two methods for de-identification under HIPAA: (1) the expert determination method, which requires an expert to apply statistical or scientific principles for rendering information not individually identifiable; and (2) the safe harbor method, which includes the removal of 18 identifiers and requires that the covered entity or business associate has no actual knowledge that the residual information can identify an individual.

A very small risk of re-identification by recipients may remain, and de-identified data can include a re-identification code that allows the covered entity or business associate to readily re-identify the information.

GDPR defines anonymized data as "data rendered anonymous in such a way that the data subject is not or no longer identifiable." Anonymized data must be stripped of any identifiable information to the point where it is basically impossible to derive insights on a discreet individual, even by the party that is responsible for the anonymization. Unlike HIPAA's de-identification standard, the hallmark of GDPR anonymization is that data should be nearly impossible to re-identify.

Breach reporting

Both GDPR and HIPAA have strict breach reporting requirements and require entities to have reporting timelines, policies, breach detection, investigation and reporting procedures in place. However, both laws have different timelines and requirements for reporting a breach. Under GDPR, a controller must report a breach of personal data no later than 72 hours after becoming aware of it to the relevant supervisory authority. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, a controller should inform affected individuals without undue delay. Processors must inform controllers of data breaches without undue delay.

HIPAA requires covered entities to report breaches of unsecured PHI without unreasonable delay and no later than 60 days following the discovery of a breach. Covered entities must notify the individuals of the breach and, if the breach affects more than 500 residents of a state or jurisdiction, provide notice to prominent media outlets serving the state or jurisdiction. Covered entities are also required to notify the US Department of Health and Human Services (HHS) of all breaches. If the breach affects 500 or more individuals, the covered entity must notify HHS without unreasonable delay and no later than 60 days after discovery. If the breach affects less than 500 individuals, then the covered entity must notify HHS by approximately March 1st of the following year.

Processing vs. uses and disclosures

Similar to HIPAA, which permits the use and disclosure of PHI if permitted by the Privacy Rule, GDPR requires controllers or processors to have a lawful basis for processing the personal data of an EU data subject. Under GDPR, the term "process" is very broad and generally covers anything that is done to the personal data (e.g., collecting, recording, organizing, structuring, storing, altering, adapting, using, disclosing, retrieving, disseminating

or making available, restricting, erasing, or destroying data).

HIPAA defines "use," as applied to PHI, to mean "the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information." Disclosure means "release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information."

Some types of uses and disclosures of PHI allowed under HIPAA are also permissible under GDPR. For example:

Consent: GDPR permits the use of health data with explicit consent from the subject. HIPAA permits the use or disclosure of PHI pursuant to an individual's authorization.

Treatment: GDPR permits the processing of sensitive personal information if necessary for the purposes of preventive or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care, 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. HIPAA permits the use or disclosure of PHI for treatment purposes, which includes the "provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another."

The compliance deadline for GDPR was May 25, 2018. The penalties for non-compliance are substantial: up to 4% of global revenue.

Required by law

GDPR permits the processing of sensitive personal information if there are 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. Under HIPAA, PHI may be used or disclosed as "required by law." Required by law is a mandate contained in a law that compels a covered entity or business associate to use or disclose PHI and that is enforceable in a court of law.

Public health

GDPR permits the processing of sensitive personal information that is necessary for public health reasons, such as preventing serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medical products or medical devices. HIPAA permits use or disclosure of PHI to public health authorities that are legally authorized to receive reports for purposes of preventing or controlling disease, injury, or disability. For example, many US states require US healthcare providers to report cases of communicable disease and vital events (e.g., death or birth).

Research

GDPR permits the processing of sensitive personal information for scientific and historical research purposes or statistical purposes. Under HIPAA, PHI may be used or disclosed for research purposes as long as it contributes to generalized knowledge and certain criteria are met.

GDPR enforcement

The compliance deadline for GDPR was May 25, 2018. The penalties for non-compliance are substantial: up to 4% of global revenue. Although the deadline has passed, it is not too late to begin compliance. EU enforcers are more likely to focus initially on entities that handle information for large numbers of EU data subjects or have particularly egregious conduct. It is less likely that initial enforcement efforts will focus on US entities that handle small amounts of EU data subjects' information.

Conclusion

GDPR represents a significant global change to the protection of privacy and security. It is changing the way companies think about privacy, and compliance can be very costly. But don't believe every headline suggesting that every US healthcare provider who treats a European tourist must comply with GDPR. Instead, take a deep breath, carefully scrutinize every nexus your organization has with EU data subjects, review the data collected on your website, and then make an educated determination as to whether GDPR applies. If you find yourself in the minority of US healthcare providers that are subject to GDPR, you will find that your HIPAA compliance program has given you a strong start. And, if you missed the GDPR compliance deadline, it is never too late to get started.

1. Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. L119.
2. 42 U.S.C. §§ 1320d—1320d-9; 45 CFR Parts 160 to 164.