Cognizant

The U.S. Healthcare Implications of Europe's Stricter Data Privacy Regulations

Domestic healthcare organizations must brush up on the EU's General Data Protection Regulation (GDPR) compliance or risk heavy fines; here's how to get started.

Executive Summary

Effective May 25, the European Union's General Data Protection Regulation (GDPR) promises to levy business-crushing fines on companies that fail to protect consumers' personal data. A wide array of U.S. healthcare organizations that market to, serve and/or employ EU residents will find themselves subject to the GDPR's provisions.

In our view, many organizations may have to go beyond their Health Insurance Portability and Accountability Act (HIPAA)-compliant measures to meet GDPR requirements. Investing in GDPR-approved technologies, such as pseudonymizing, will enhance healthcare organizations' overall data security and privacy, as this white paper recommends.

GDPR: HIPAA ON STEROIDS

The U.S. healthcare industry is well acquainted with privacy and security regulations, mainly in the form of HIPAA. Yet the GDPR, designed to protect the data and privacy of individual European Union citizens, makes HIPAA look tame in comparison. U.S. healthcare organizations that collect data on EU citizens, whether they are customers or employees, are likely to face strict GDPR enforcement – and not just for health data.

The GDPR replaces older EU privacy legislation (see Figure 1). It applies to all companies that collect, store and process information about individuals in EU countries, even if the companies themselves are not headquartered in Europe. The regulation sets much higher penalties for corporate noncompliance than previous statutes – up to 4% of a company's total global revenues.

To put that 4% into context: In 2016, the UK's Information Commissioners Office (ICO) fined

Evolving EU Personal Data Protection Legislation

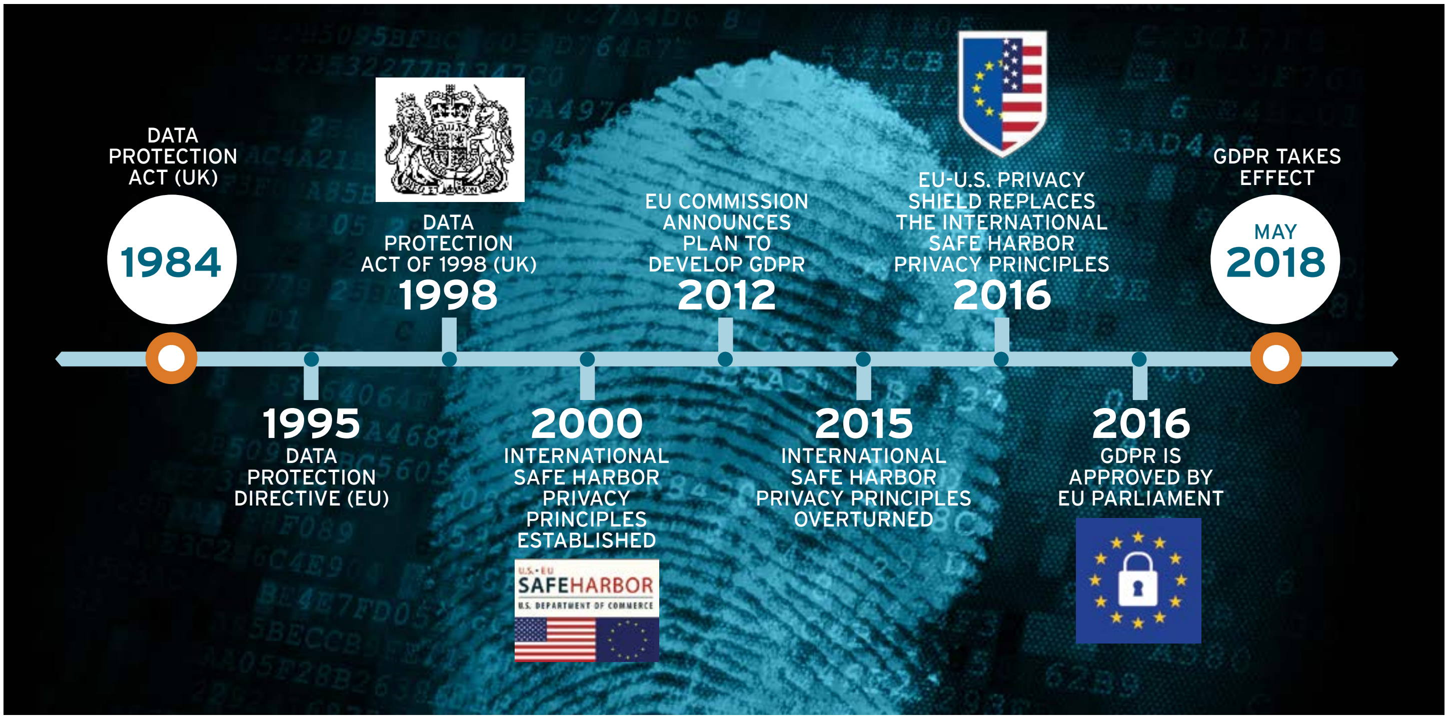
DATA PROTECTION ACT (UK)
1984
DATA PROTECTION ACT OF 1998 (UK)
1998
EU COMMISSION ANNOUNCES PLAN TO DEVELOP GDPR
2012
EU-U.S. PRIVACY SHIELD REPLACES THE INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES
2016
GDPR TAKES EFFECT
MAY 2018
1995
DATA PROTECTION DIRECTIVE (EU)
2000
INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES ESTABLISHED
U.S.-EU SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE
2015
INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES OVERTURNED
2016
GDPR IS APPROVED BY EU PARLIAMENT

Figure 1

Talk Talk, a British communications provider, £400,000 ($560,000) after it determined security failings allowed a cyber-attack to access the company's customer data "with ease."[1] Under GDPR, Talk Talk's fine would have been £59 million ($82.7 million) — a nearly 1,500% increase.

Overall, fines against UK companies in 2016 would have skyrocketed from £880,500 ($1.23 million) to £69 million ($96.7 million) if GDPR had applied that year.[2]

Fines like these, and EU member countries showing a willingness to investigate the privacy and security practices of U.S.-based companies operating physically or virtually within their borders, should create some urgency among domestic healthcare organizations for ensuring they are GDPR compliant. Industry organizations affected include international healthcare, medical supply and life sciences companies; health analytics companies; international pharmacy benefit managers; payers; and healthcare providers.

Broader and Deeper than HIPAA

The GDPR calls for higher protection standards for health data and delineates a variety of definitions and conditions that apply to such data (see sidebar, page 4). The regulation creates three main categories for health data:

- **Data concerning health:** This is defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

- **Genetic data:** The regulation defines this as "personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."

- **Biometric data:** The GDPR definition is "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or [fingerprint] data."

Under GDPR, this health data may be processed only under three specific conditions:

- The subject must give "explicit consent" to the data processing. Explicit consent must be unambiguous — a clear affirmative statement or action of the subject to agree to the processing.

- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, for a medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services.

- Processing is necessary for reasons of public interest in the area of public health, such as protection 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.

The GDPR clearly differs from HIPAA in its scope and intent, with GDPR designed to help individuals gain more control over how their complete digital data trails are used, by whom and for how long (see Figure 2, page 5) vs. regulating a single industry.

QUICK TAKE

What GDPR Requires

In addition to basic conditions for data collection and processing, the GDPR spells out other requirements companies handling data on EU citizens must meet. These include:

- **Data protection officer (DPO):** Organizations that engage in large-scale monitoring and processing of sensitive personal data must appoint DPOs (Art. 37).[3]
- **Right to data portability:** Requires entities to send personal data back to the data subjects for them to transmit it elsewhere more easily.
- **Right to be forgotten:** Requires entities to erase personal data without "undue delay."
- **Subject access right (SAR):** Allows subjects to gain access to their personal data free of charge and within a month of the request.
- **Right to not be subject to profiling:** Allows subjects to opt out of profiling activities.
- **Right not to use data beyond its original purpose:** Data must not be accessed for any purpose other than the intended use.
- **72-hour breach reporting:** Breaches including health data are automatically considered "likely to result in high risk" and must be reported within 72 hours.
- **Contract/agreement renegotiations:** Existing vendor contracts and statements of work must be renegotiated before May 2018 to incorporate the provisions required by the GDPR. New contracts must include the required provisions.
- **Data privacy impact assessments (DPIAs):** Will be required when using new technologies and for any data deemed "high risk" to the rights and freedoms of individuals.
- **Compliance:** Companies must demonstrate compliance with its GDPR obligations. They need to maintain extensive records and documentation, as ongoing monitoring and audits will be required.
- **Training:** All associates involved in data processing, potentially including clinicians, must be educated as they share the responsibility of the law.

> GDPR is designed to protect the fundamental rights and freedoms of data subjects, address data processing in the light of digital advances and streamline data protection laws across the EU. By contrast, HIPAA is designed to prevent unauthorized data access within a healthcare ecosystem vs. addressing broader digital trust and data ownership issues.

The GDPR is designed to protect the fundamental rights and freedoms of data subjects, address data processing in the light of digital advances and streamline data protection laws across the EU. By contrast, HIPAA is designed to prevent unauthorized data access within a healthcare ecosystem vs. addressing broader digital trust and data ownership issues.

A Study in Compliance: Comparing GDPR to HIPAA

	GDPR	HIPAA
Intent	Protect the fundamental rights and freedoms of data subjects. Enable the free movement of personal data within the EU. Contribute to economic and social progress and trade. Address the processing of personal data in light of technological progress. Harmonize data protection laws across the EU.[4]	Ensure the security and confidentiality of patient data and information. Mandate uniform standards for electronic data transmission of administrative and financial data relating to patient health information.
Scope	Legislation applies to all industry sectors.	Healthcare sector.
Geography	Protects EU residents. It applies to goods and services offered to EU residents or when the behavior of EU residents is monitored.	Protects US residents' health information.
Scale	Same rules apply to all types and sizes of organizations.	Health plans, healthcare clearinghouses, health providers.
Type of Data	Personal data (i.e., name, date of birth, pseudonymous data, are treated as personal). Sensitive personal data (i.e., genetic data, biometric data).	Individually identifiable health information (PHI and EPHI).
Fines	20 million Euros or 4% of total global revenues – whichever is larger.	Civil penalties: $100 to $1.5M annual maximum. Criminal penalties: up to $250K, up to ten years imprisonment.
Breach Notification Time Frame	72 hours.	60 days after breach.

Figure 2

The GDPR specifically recommends two security techniques, encryption and pseudonymization. While HIPAA requires data in transmission to be encrypted, it calls encrypting data at rest (in storage) an "addressable" vs. "required" practice. The GDPR's endorsement of this sound practice should give the industry more impetus to widely implement it.

HIPAA ensures the security and confidentiality of patients' data and mandates standardization of data transfers regarding protected health information (PHI). HIPAA requires that PHI only be accessed and/or used for "treatment, payment, and operational" needs, including research, if that intent is disclosed at the time of collection and data is de-identified.[5]

However, HIPAA puts the onus on the patient to discover who has accessed health records and to inform organizations about who may not see health data. In comparison, GDPR requires more explicit and active consent and individuals can ask for in-depth descriptions of how their data is being processed, and receive the data in an electronic copy that they may then transfer to another party, among other rights.

Due to these distinctions, systems and policies supporting HIPAA are narrower in scope and do not automatically ensure GDPR compliance.

TECHNOLOGY FOR GDPR COMPLIANCE

Any technology investments required to support GDPR also should help make PHI and other data more secure. That's not a small consideration, given that the U.S. healthcare industry has a poor record of preventing data breaches, with more than three million records affecting more than 14 million individuals exposed in 2017 alone.[6] Further, the GDPR requires breaches of such data to be reported in 72 hours; HIPAA allows up to 60 days.

The GDPR specifically recommends two security techniques, encryption and pseudonymization.[7] While HIPAA requires data in transmission to be encrypted, it calls encrypting data at rest (in storage) an "addressable" vs. "required" practice.[8] The GDPR's endorsement of this sound practice should give the industry more impetus to widely implement it.

Pseudonymization is a procedure in which identifying fields within a data record are replaced by one or more artificial identifiers, i.e., pseudonyms, so that the data cannot be linked to an identity without additional information. A single pseudonym might replace a collection of data fields or a single field. The purpose is to render the data record owner less identifiable and therefore assuage customer or patient objections to its use. The advantages under GDPR to pseudonymization:

- Data in this form is suitable for extensive analytics and processing.[9]
- The GDPR relaxes several requirements on entities that use pseudonymization.[10] Such organizations will be able to use personal data for secondary purposes such as “general analysis” more easily if they pseudonymize the data – as long as the processing organization has specific, fully informed and active consent; neither prefilled boxes nor silence is to be taken as assent.[11] Data subjects also have the right to refuse or withdraw consent.

Pseudonymization can be weak against inference attacks. Protecting statistically useful pseudonymized data from re-identification requires a sound informational security base and minimizing the risk that analysts, researchers or other data workers can cause a privacy breach.

The GDPR also recommends using encryption, a technique that encodes data so that only authorized individuals holding an encryption key generated by an algorithm may decrypt it.

Encryption vs. Tokenization

ENCRYPTION	TOKENIZATION
Mathematically transforms plain text into cipher text using an encryption algorithm.	Randomly generates a token value for plain text and stores the mapping in a database.
Scales to large data volumes with just the use of a small encryption key to decrypt data.	Difficult to scale, secure and maintain performance as database size increases.
Used for structured fields, as well as unstructured data such as entire files.	Used for structured fields such as payment card or Social Security numbers.
Ideal for exchanging sensitive data with third parties who have the encryption key.	Difficult to exchange data because it requires direct access to a token vault mapping token values.
Format-preserving encryption schemes come with a tradeoff of lower security strength.	Format can be maintained without diminished security strength.
Original data leaves the organization but in encrypted form.	Original data never leaves the organization, satisfying some compliance requirements.

Figure 3

> The DPO will establish governance and oversight for the implementation of GDPR across the enterprise. The role requires a person with a solid data management and security background, business acumen and human capital development abilities to build and grow an effective cross-functional and interdisciplinary GDPR team.

That said, tokenization may be a better alternative than encryption because after files have been encrypted, it is nearly impossible for employees to work with them.[12] (See Figure 3, previous page, for a comparison of the key features of encryption and tokenization.) Tokenization replaces personal identifiers with random codes; employees work with data anonymized with tokens much more easily than encryption. It does require a master table that maps codes to identifiers; the security downside is that the master table could be captured in a data breach. Tokenization is now being used to protect data to maintain the functionality of back-end systems without exposing personally identifiable information to attackers.

Blockchain is another potential solution.[13] Blockchain creates a continuously growing list of records, or blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a time stamp and transaction data. The fact that a blockchain is a permanent ledger makes it inherently resistant to data modification. Once recorded, the data in any given block cannot be altered retroactively without altering all the subsequent blocks, which would require the collusion of most or all the participants in the blockchain. (For more on blockchain's healthcare potential, read "Healthcare: Blockchain's Curative Potential for Healthcare Efficiency and Quality."

WHAT TO DO RIGHT NOW

The time to deal with the GDPR from policy, process and system perspectives is now, not when an EU regulator announces an investigation into how U.S. healthcare companies are gathering data on EU citizens. Here are some steps to take right away:

- **Identify why your organization needs to align with GDPR.** Consult your organization's compliance department and/or legal counsel about the areas in which the organization could already be noncompliant, or do so as it rolls out different business ventures focused on EU nations.

- **Next, an enterprise must evaluate organizational change.** This starts with identifying roles, responsibilities and skills needed to form a GDPR compliance team. Having a data protection officer (DPO) to spearhead the initiative is mandatory. The DPO will establish governance and oversight for the implementation of GDPR across the enterprise. The role requires a person with a solid data management and security background, business acumen and human capital development abilities to build and grow an effective cross-functional and interdisciplinary GDPR team.

GDPR compliance will mean revisiting data collection, processing and storage strategies with a fresh approach. While no simple task, the effort will yield improvements in protection of personal data and privacy, faster and more effective responses if breaches occur and an overall increase in patient trust.

- **The GDPR team first must plan the GDPR initiative and create the implementation roadmap.** During this process, it is critical to develop a standard toolkit of prebuilt methods, tools and templates to launch the initiative. Clear problem-solving, accountability and decision-making systems must be put in place at this point for successful program execution.

- **The project team must evaluate the organization's current data architecture, including pseudonymization, anonymization, obfuscation, data masking and encryption capabilities.** It must also develop the future state vision to identify gaps in GDPR compliance readiness.

- **The GDPR team must inventory IT platforms (important for large organizations) and their economic life.** Ineffective platforms that don't meet security and privacy levels for data must be either upgraded or replaced.

- **Finally, the team must design business processes that need to be embedded in current workflows to ensure GDPR compliance.**

For healthcare organizations, GDPR compliance will mean revisiting data collection, processing and storage strategies with a fresh approach. While no simple task, the effort will yield improvements in protection of personal data and privacy, faster and more effective responses if breaches occur and an overall increase in patient trust.

All healthcare organizations will require these qualities as healthcare becomes increasingly digital; it's not farfetched to assume healthcare consumers will rate healthcare organizations on trust and data security as healthcare transactions become digitized.

ABOUT THE AUTHORS

Vanessa Pawlak

Practice Leader, Regulatory Compliance and Government Programs, Healthcare Practice, Cognizant Consulting

Vanessa Pawlak is the Regulatory Compliance and Government Programs Practice Leader in Cognizant Consulting's Healthcare Practice. She has more than 15 years of consulting experience and has worked with all 10 of the largest U.S. payers, 17 Blues organizations, state health agencies and more than 70 health organizations across the country. Vanessa is board certified in health compliance and health data privacy. She specializes in government-sponsored health programs, with experience directing large-scale transformation and turnarounds across governance/administration, operations, financial and clinical domains. Vanessa may be reached at Vanessa.Pawlak@cognizant.com.

Octavia Costea

Manager, Regulatory Compliance and Government Programs, Healthcare Practice, Cognizant Consulting

Octavia Costea is a Manager in the Regulatory Compliance and Government Programs Practice within Cognizant Consulting's Healthcare Practice. She has 15 years of experience in payer, provider and government programs, focusing on payment and reimbursement reform and compliance. Octavia is scaled Agile-certified (SA) and has an MBA from Babson College, and an MA and JD from "P. Andrei" University, Romania. She is also Board Certified in Radiology Technology (Nuclear), RT(N). Octavia can be reached at Octavia.Costea@cognizant.com.

ACKNOWLEDGMENTS

The authors would like to thank Steve Rounds, a Senior Consultant in Cognizant Consulting's Healthcare Practice, for his contributions to this white paper.

FOOTNOTES

[1] Information Commissioner's Office, October 5, 2016, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/.

[2] NCC Group, April 28, 2017, www.nccgroup.trust/us/about-us/newsroom-and-events/press-releases/2017/april/last-years-ico-fines-would-soar-to-69-million-post-gdpr/.

[3] "GDPR FAQs" EU GDPR Compliant, www.eugdpr.org/gdpr-faqs.html.

[4] Dr. Detlev Gable and Tim Hickman, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law; Chapter 3, White & Case LLP, July 22, 2016, www.whitecase.com/publications/article/chapter-3-subject-matter-and-scope-unlocking-eu-general-data-protection.

[5] Office for Civil Rights, December 18, 2017, www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.

[6] HIPAA Journal, January 4, 2018, www.hipaajournal.com/largest-healthcare-data-breaches-2017/.

[7] Gabe Maldoff, International Association of Privacy Professionals, February 12, 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/.

[8] "HIPAA Compliance Checklist 2017-2018," HIPAA Journal, www.hipaajournal.com/hipaa-compliance-checklist/.

[9] "Pseudonymization," Wikipedia, https://en.wikipedia.org/wiki/Pseudonymization.

[10] ibid, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/.

[11] Dr. Detlev Gable and Tim Hickman, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law; Chapter 8, White & Case LLP, July 22, 2016, www.whitecase.com/publications/article/chapter-8-consent-unlocking-eu-general-data-protection-regulation.

[12] Laura Vugh, "Encryption vs. Tokenization. Which is better and when to use them?" EU GDPR Compliant, January 30, 2017, https://eugdprcompliant.com/knowledgebase/encryption-vs-tokenization/.

[13] "Blockchain," Wikipedia, https://en.wikipedia.org/wiki/Blockchain.

ABOUT COGNIZANT

Cognizant (NASDAQ-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 205 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

Cognizant®

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

TL Codex 3542