The MPI Group
People. Purpose. Profits.

Healthcare and the GDPR

New Standards, New Risks — and New Opportunities

Brought to you by Canon U.S.A., Inc.

Canon

www.cusa.canon.com

Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPPA) established national standards for the security of health information that is collected or processed by covered entities and their business associates in the United States, with significant penalties for violations.[1] HIPPA required major changes in the management of personal information among healthcare providers, helping to usher in a new era of electronic information systems and security technologies.

Yet HIPAA was only the beginning. With the enactment of the General Data Protection Regulation (GDPR) in the European Union, healthcare organizations may be challenged to further improve their collection and handling of personal information. Yet amid general concern and uncertainty in the sector about GDPR compliance, some organizations see opportunity.

Why?

Because leaders at these organizations understand that streamlined information workflows can not only enhance security and GDPR compliance efforts, but also help them to serve their patients better and deliver a competitive edge. With best practices and technology-enhanced information workflows, healthcare organizations can become more responsive, agile, and efficient — and create models for personal information management that may serve them for years to come.

New Standards and New Risks

Healthcare organizations hold vast amounts of private information, some of which may be subject to the purview of the GDPR, including:

- EU patient care records
- EU patient billing records
- EU pharmaceutical records
- EU physician and staff records
- Job applications from EU individuals
- Healthcare portal/website access information
- Research and clinical trial data containing EU personal data
- Communications with — and marketing to — EU subjects (website, email, Facebook, etc.).

In response to individuals' demands for greater control over their information and who holds and uses it, other privacy-rights regulations are also emerging around the globe, some of which mimick the intent and power of GDPR. The array of penalties that governments can impose on healthcare organizations to protect personal information has increased as well.

With best practices and technology-enhanced information workflows, healthcare organizations can become more responsive, agile, and efficient — and create models for personal information management that will serve them for years to come.

[1] "Summary of the HIPAA Security Rule," U.S. Department of Health and Human Services.

After decades in the making and a two-year period for organizations to prepare, on May 25, 2018 the European Union began enforcement of the GDPR. Some consumers and privacy rights activists argue that laws such as GDPR are long overdue, with regulators lagging behind technological advances. This means that while GDPR compliance may seem daunting now, tomorrow it may be viewed as just another cost of doing business in the EU — or anywhere.

GDPR covers the "protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data,"[2] and dramatically increases personal-data security responsibilities and risks for businesses of all types *(see GDPR Basics)*. Even more significant is GDPR's establishment of new standards for data privacy rights that other lawmakers may replicate. For example, in June 2018, California passed a digital privacy law, effective January 1, 2020, that gives consumers more control over their personal information online.[3] And as inappropriate uses of personal data by holders and hackers continue to make news, increasingly stringent regulations may be likely.

The California Consumer Privacy Act reflects the intent of lawmakers to regulate data-collection and -sharing practices, and illustrates how important it is for U.S. organizations to comply with emerging global standards (i.e., GDPR) — and that includes healthcare organizations.

While healthcare organizations may be better prepared for GDPR than other sectors due to HIPPA compliance efforts, many have failed to keep personal information secure. In fact, 110 health data breaches were disclosed to the U.S. Department of Health and Human Services (HHS) or the media from January to March 2018. Details were disclosed for 84 incidents, affecting more than 1 million patient records.

With or without the requirements imposed by GDPR, one thing is certain: breaches are likely to be more costly in the future, given that penalties for violating GDPR data security regulations are severe (and potentially far more significant than HIPPA penalties). Fines for GDPR non-compliance, for example, can reach €20 million or up to 4 percent of an organization's annual worldwide revenue of the preceding financial year, whichever is greater.[4]

While compliance *risks* grab much of the attention around GDPR and other regulatory changes, *opportunities* for healthcare organizations abound as well. Many of the new processes and new technologies that may improve data security and GDPR compliance efforts may also help to streamline document workflows in ways that help to improve patient care, boost efficiency, and reduce costs.

[2] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

[3] California Consumer Privacy Act, caprivacy.org.

[4] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

GDPR Basics[5]

The GDPR replaced Data Protection Directive 95/46/EC, and is intended to harmonize data privacy laws across EU member states. It assigns control of personal data to individuals in the EU and incorporates an array of new rights for EU data subjects, including the right to:

Access information about personal data: An EU data subject has the right to obtain from data controllers confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to such personal data. Such EU data subjects can also have the right to obtain information on, among other things, the purpose of the processing, the categories of personal data, the recipients or categories of recipient to whom personal data has been disclosed, etc.

Be forgotten: An EU data subject has the right to obtain from controllers the erasure of personal data concerning him or her, without undue delay, and controllers are obligated to erase personal data without undue delay, if certain circumstances apply.

Automated individual decision-making, including profiling: An EU data subject has the right to not be subject to a decision based solely on automated processing, including profiling. The law regulates, among other things, the profiling of a person for the purpose of analyzing or predicting the individual's personal preferences, behaviors, and attitudes.

Consent: Unless expressly allowed by law, an EU data subject's personal data cannot be processed without his or her consent. Consent must be freely given, specific, informed, via an unambiguous indication of the EU data subject's agreement to the processing of personal data (e.g., by a written statement, ticking a box when visiting an internet website). Pre-ticked boxes or inactivity do not constitute consent.

Data portability: An EU data subject has the right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, machine-readable format, and has the right to transmit the data to another controller, if certain circumstances apply.

[5] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Time limits: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

GDPR is likely to alter the ways healthcare organizations collect and manage personal information. It defines and may require "data controller" and "data processor" roles for organizations dealing with EU data subjects, and identifies required processes that may apply to both (appointment of a "data protection officer," response to a breach, etc.):

Controller is the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of the processing of personal data. The controller implements appropriate technical and organizational measures to ensure and demonstrate that data processing is performed in accordance with GDPR, including application of data-protection policies.

Processor is the natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. Processors need to meet the standards set forth by controllers. Where processing is done for a controller, the controller needs to ensure that the processor has sufficient guarantees to implement appropriate technical and organizational measures to comply with GDPR and can ensure the protection of the rights of EU data subjects.

Data protection officer: Controller and processor shall designate a data protection officer in any case where processing is carried out by a public authority or body, except for courts acting in their judicial capacity; the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 of the GDPR and personal data relating to criminal convictions and offenses referred to in Article 10 of the GDPR.

Lastly, and of importance to U.S. healthcare organizations, GDPR extends to foreign organizations processing the data of individuals in the EU. For example, if a patient or employee is located in the EU, all EU personal data handled by the U.S. healthcare provider can be subject to the GDPR. Non-EU established businesses are subject to the GDPR where they process personal data of data subjects in the EU in connection with behavior of individuals in the EU.

Catching Up to GDPR

The GDPR is a complex set of regulations; it's no wonder that more than two years after the EU approved them in April 2016, compliance challenges may remain for many healthcare organizations, including:

- Addressing accountability requirements — both compliance and proof of compliance are required
- Documenting data-management protocols and processes (i.e., information workflows)
- Reviewing data-collection procedures to ensure consent
- Proving the necessity of processing personal data, if and when collected
- Securing vulnerable systems against a range of cyberthreats (malware, ransomware, etc.)
- Establishing procedures to quickly report breaches.

Even worse, many U.S. healthcare organizations may be unaware of the full extent of the GDPR and its impact. For example, in the pharmaceutical sector, only 54 pecent of North Americans in the industry surveyed felt informed about the new EU regulation, compared to 82 percent of Europeans and those in the Asia-Pacific (APAC) region, and 67 percent of those in other regions.[6]

Exposure to GDPR does not require *physically* conducting business in the EU or providing healthcare services into the EU; mere *holding of data* on EU individuals is also covered under GDPR. U.S. healthcare organizations must establish policies and infrastructures that meet the GDPR thresholds for information they likely hold.

One study found that between 43,000 and 103,000 foreigners annually came to the United States for medical care;[7] others estimate the figures to be two or three times higher. Many hospitals and academic medical centers also extend their expertise into other countries, "collaborating with overseas healthcare organizations to advance healthcare abroad and strengthen health infrastructure and access."[8] Connections to international patients or research increase the likelihood of EU personal data moving through U.S. healthcare organizations.

[6] "North Americans Are The Least Informed About GDPR In Pharma, Says GlobalData," *Clinical Leader,* Aug. 9, 2018.

[7] Tricia J. Johnson and Andrew N. Garman, "Impact of medical travel on imports and exports of medical services," *Health Policy,* December 2010.

[8] Teresa L. Johnson, "U.S. Hospitals with International Patients Enter Overseas Improvement Projects," *Global Healthcare Insights,* Sept. 28, 2017.

Minimize GDPR Risks

Healthcare organizations capturing and holding EU personal data should know what data is collected; why data is being collected; where data is held and processed; and who has access. Despite consolidation of data into electronic health records (EHR) systems, some healthcare leaders are challenged to find these answers — in legacy systems, paper-based records, and varying software applications among satellite locations, partners, and affiliates. To meet GDPR requirements, healthcare organizations typically develop data-centric strategies for which all departments, functions, and technology platforms contribute to a solution (i.e., no rogue plans) with role-specific objectives and GDPR activities:

- *The organization:* The organization should have an overall strategy based on a review of where personal data is held (systems) and its ability to manage this information in ways compliant with GDPR. An organization-wide strategy establishes GDPR awareness, requirements, and enforcement methods for all functions and departments.
- *Information technology (IT) departments:* IT departments should have develop technical strategies that align with those of their organizations, possibly integrating new systems and networks with legacy technologies to accommodate personal data requirements and requests; improve security; and deploy breach-awareness capabilities. IT also plays a key role in data governance and systems strategies.
- *Procurement:* The organization must develop or refine guidelines and support contracts to minimize GDPR-compliance risks associated with partners and vendors for care services (non-staff physicians, outpatient services); goods (systems, applications, office devices); and other services (data processors, hosting firms).

The organization and all parties involved with it can take steps to minimize risks of GDPR non-compliance *and* streamline personal information workflows by, among other things:

Understanding why data is collected, and where it's kept

It's important for healthcare organizations to document *why* they collect any piece of personal information from EU data subjects, *what* they do with it, and to *whom* it is disclosed — even if the organization did not collect the information in the first place (i.e., it was provided by other organizations). Despite EHR, many U.S. healthcare organizations may have legacy information-management practices that struggle to achieve common needs, let alone GDPR compliance: limited or missing authorizations for information; non-standardized information collection and handling processes; mixed file formats that make data searches inefficient or impossible, etc.

At the same time, the volume of data collected in healthcare is growing dramatically — rising from 153 exabytes in 2013 to a projected 2,314 exabytes in 2020.[9] Making matters worse, many organizations still have complex, siloed information workstreams with poor processes, overreliance on paper documents, and incomplete documentation.

Even where a hospital's main campus has consistent practices and processes for managing information, there's no guarantee that offices of associated physicians and specialists follow those same rules; even meeting EHR requirements can be a daunting task for off-site physicians and their employees. Mapping information workstreams is a good first step for healthcare organizations to track the collection and processing of personal information, as well as adherence to GDPR compliance requirements.

While there is no specific GDPR requirement for data mapping itself, this exercise can be a key component of compliance.[10] Why? Because mapping can help to identify *where* personal information is kept (e.g., systems, contact lists, email addresses) and to optimize *how* this information is managed in ways consistent with GDPR. For example, do the location and access provisions for a specific type of data make it easy to find and revise or delete records upon request? Can the healthcare organization identify and remove unnecessary personal information — across all functions, departments, and offices?

Just as important, data mapping can identify delays and waste in document management processes — enhancing collaboration, productivity, and organization performance.

Accommodating customized data requirements

The GDPR's right of information and access to personal data grants EU data subjects the right to information about data collected about them, and gives data subjects information necessary to assess whether processing is fair and transparent.[11] To do this, healthcare organizations should consider the implementation of personal-data workflows that can improve compliance efforts with respect to GDPR requirements; automating these new processes can help administrators in meeting EU data subject requests.

Even where a hospital's main campus has consistent practices and processes for managing information, there's no guarantee that offices of associated physicians and specialists follow those same rules.

[9] *Stanford Medicine 2017 Health Trends Report: Harnessing the Power of Data in Health,* citing International Data Corp. research, June 2017.

[10] Alison Cregeen, "A practical guide to data mapping for GDPR compliance," PWC, March 6, 2018.

[11] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Developing consistent, enterprise-wide, information-governance strategies

All actions involving personal data — collecting, hosting, managing and sharing patient records, removing data, working with support vendors, etc. — must be aligned with organization-wide GDPR strategies, policies, and technologies, from main campuses out to affiliated units — for example, regional centers and physician offices for hospitals, or branch locations for a pharmacy chain. Even if a healthcare organization is defined solely as a data controller for a given data set (i.e., it collected and defined how the data is to be used and processed), it should ensure that its data processor(s) are GDPR compliant, too.

Ideally, healthcare organizations will have taken steps to become GDPR-compliant long before May 2018, such as:

1. Assembling a cross-functional working group to review and assess GDPR and its impact on the organization.
2. Conducting data mapping of personal information workstreams and assessment of GDPR-compliance gaps (e.g., potential for unauthorized access, inability to quickly remove or alter data, unauthorized collection of unnecessary personal information).
3. Establishing policies and governance around GDPR data management.
4. Trialing new practices in model areas (e.g., office, department) to test GDPR risk exposure and compliance.
5. Communicating GDPR policies and procedures throughout the organization and assembling and deploying subgroups as necessary to implement new practices.
6. Routinely reassessing GDPR risk exposure and compliance.

Leverage Opportunities in GDPR Compliance

Some improvement-minded financial institutions are changing their data processes, workflows, and document-management systems to improve data security — but with other gains in mind, too. Indeed, for some, GDPR compliance is a vehicle to leverage data workflow improvements to enhance day-to-day operations and bring greater value to customers, staff, and stakeholders. This is done by implementing new best practices, new work models, and new technologies that impact:

- *Data workflows:* Lean healthcare organizations — those seeking to continuously remove waste and costs and add value for patients and customers — have used process mapping for years to identify bottlenecks and wastes that can drain profits even as they frustrate patients, partners, and staff. Mapping can not only define new document workflows that can help to address GDPR requirements but can also help to streamline *all* document workflows. For example, moving from paper or mixed-media information formats to all-digital data workflows can improve the overall efficiency of office operations, which can deliver financial benefits.

  Mapping can also identify gaps in security and information controls, which can allow users to understand how to remediate potential security liabilities and establish a log of activities through which personal information travels, from handling to authorized access.

- *Data security:* Healthcare organizations can implement new personal data workflows with automated tracking mechanisms to document collection and management. Data protection technologies can be integrated into processes to help minimize the risk of security breaches, such as incorporating protected and/or sensitive content into regulated workflows as soon as data is received; limiting unauthorized access to office devices; and ensuring that digital communications leverage classification tools to help users accurately catalog, store, and protect information.

Some improvement-minded healthcare organizations are changing their data processes, workflows, and document-management systems to improve data security — but with other gains in mind, too.

- *Data-breach response:* GDPR will drive many healthcare organizations to limit data access (including printers, copiers, scanners, smart phones, and other touchpoints) in order to help limit breaches. And because GDPR requires that a breach be reported to authorities within 72 hours of discovery — along with identifying both the cause and likely consequences[12] — automated GDPR-alert capabilities and proactive procedures can help. New technologies that alert administrators automatically of words used or actions taken that may indicate a breach can help to compile an investigative trail, by capturing log-in information, data, and images from office devices, etc. These plans and technologies also can help healthcare organizations in contacting other authorities, business partners, and individuals regarding security breaches that may not involve GDPR and EU data subjects.

- *Deploy and model new best practices and technologies:* Healthcare organizations can embrace the GDPR as a means to prepare themselves for a new era of personal-information management. Protecting personal information privacy by establishing new infrastructure and policies may not only improve data security but also may enhance efficiency across the organization. This also can provide a template to share with those supporting the healthcare organization for managing the persondal information within their organizations — involving EU data subjects and others — and to apply to new units, centers, and offices as an organization expands.

U.S. healthcare organizations are already on the frontline of protecting personal information; GDPR raises the stakes even higher. Is your healthcare organization ready for a brave new world of data risk — and opportunity?

Protecting personal information privacy by establishing new infrastructure and policies will not only improve data security but enhance efficiency across the organization.

[12] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Canon U.S.A. is not engaged in the rendering of professional advice or services including, without limitation, legal or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the suggestions discussed in this white paper. Canon USA does not make any warranties concerning the accuracy or completeness of the opinions, data and other information contained in this content and, as such, assumes no liability for any errors, omissions or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data or other information.

Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, GDPR, Sarbanes-Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

Prepared as of 2.8.19. Rules and regulations may change from time to time. As stated above, please have your own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.