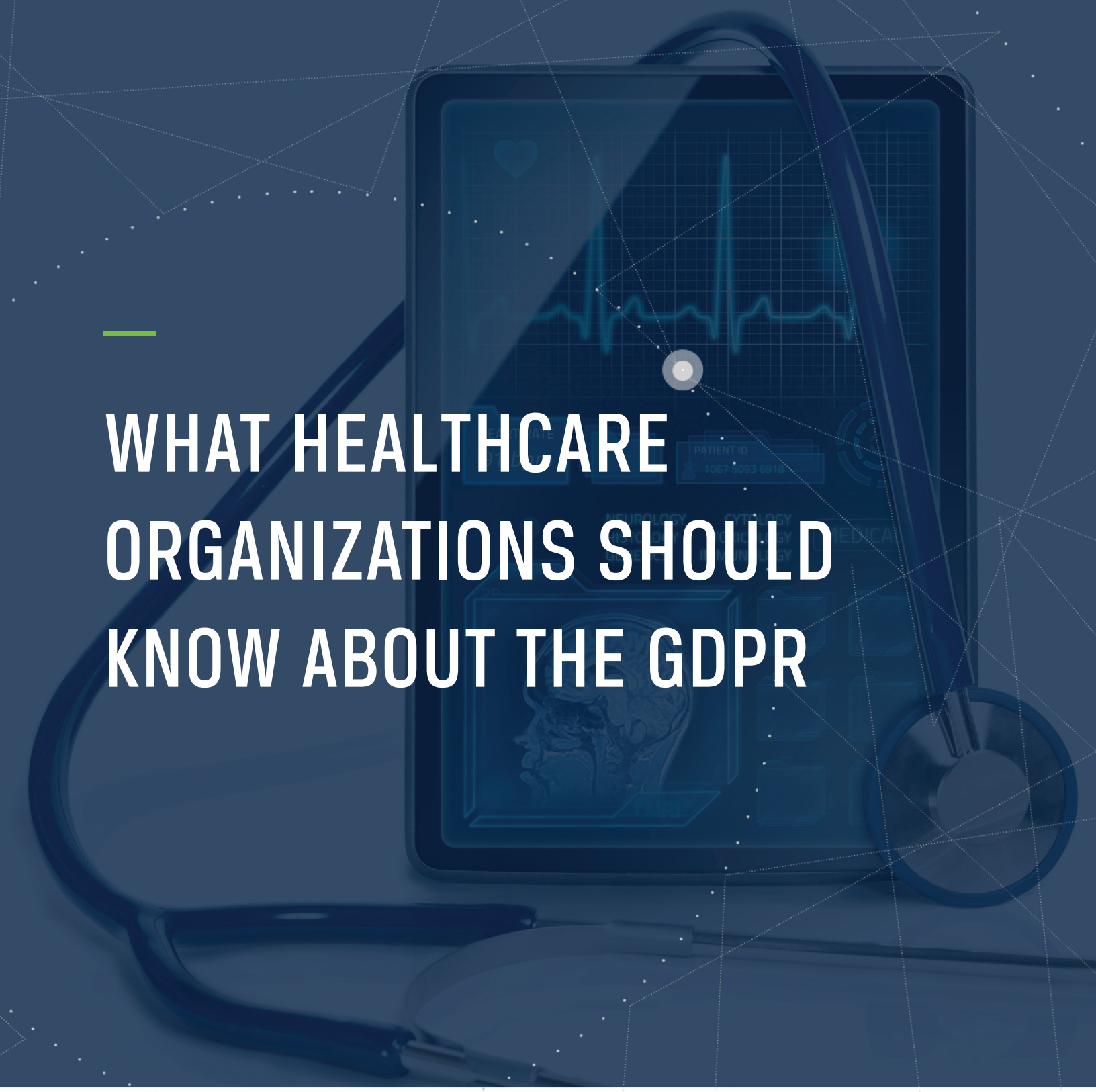

WHAT HEALTHCARE ORGANIZATIONS SHOULD KNOW ABOUT THE GDPR

ABSOLUTE

HEALTHCARE WHITEPAPER

THE HEALTHCARE INDUSTRY IS FACING MULTIPLE CHALLENGES WHEN IT COMES TO PROTECTING SENSITIVE DATA. HERE'S AN OVERVIEW OF HOW THE RECENT EU GENERAL DATA PROTECTION REGULATIONS (GDPR) WILL AFFECT HEALTHCARE ORGANIZATIONS…

INTRODUCTION

Data protection regulations define how an individual's personal information can be used by organizations, businesses and government. These regulations also contain safeguards that seek to ensure healthcare data is not susceptible to attack, misuse or misappropriation. As most know, misusing an individual's healthcare data or not properly following regulation guidelines can hold especially serious long-term consequences.

This spring, the GDPR was adopted with the aim of having one set of rules applicable throughout the European Union (EU). This has significant implications not only for EU-based organizations, but also for non-EU based organizations that conduct business or business communications in EU countries. Additionally, several instances within the GDPR allow for EU Member States to introduce specific national provisions that affect a range of sectors, including healthcare.

The GDPR further aims to ensure privacy by design or default, meaning that data protection measures must be implemented across all data processing activities and endpoints. These changes are not revolutionary; the key principles, concepts and themes of the current data protection system remain. The new rules build on what is already in place with the addition of several new requirements. Although the new rules will not formally be introduced until May 2018, what they require should compel organizations to begin preparing now.

The content that follows highlights the key changes to data protection and security compliance that the GDPR brings to the healthcare sector. Within the text, we will share several technical terms which appear in data protection legislation—for example, "data controller," "data processor" and "data processing." As needed, definitions of these terms can be found at **http://www.corderycompliance.com/eu-dataprotection-regulation-glossary/**.

WHO IS AFFECTED?

As noted above, anyone in the EU who controls data and/or undertakes data processing will be bound by the GDPR. This includes the healthcare sector and also affects organizations based outside the EU. Additionally, the GDPR holds extended responsibilities and obligations for data controllers and processors.

Controllers will have to establish or amend technical and organizational measures to ensure and prove that the processing of personal data fully complies with GDPR requirements. The way in which data protection policies are implemented will be significant here.

Processors will be required to maintain records of all their processing activities and maintain disclosure readiness of this information to show compliance. Further, processing on behalf of a controller must be set out in a contract or other "legal act," according to criteria articulated under the GDPR.

The healthcare sector will therefore have to undertake a more holistic approach to data management. If done properly, the burden will be mitigated by the reward of knowing where data is and where it goes, thereby enabling good compliance practice and reduced risk.

HEALTH DATA - A HIGHER PROTECTION STANDARD

Data concerning health has special mention under the GDPR. It defines "personal" data as "any information relating to an identified or 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 or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Further, the GDPR contains three additional important definitions that pertain to health data:

1. "Data concerning health" is defined by the GDPR 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."

2. "Genetic data" is defined by the GDPR 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."

3. "Biometric data" 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 dactyloscopic data."

What is important to highlight here is that "data concerning health," "genetic data" and "biometric data" will be subject to a higher standard of protection than personal data in general. The processing of these three forms of health data is prohibited unless one of several conditions applies.

These health-specific conditions are as follows:

1. The data subject must have given "explicit consent" (see below for the definition of consent) to the processing.

2. "Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services [...]."

3. "Processing is necessary for reasons of public interest 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 [...]."

It is important to emphasize the word "necessary" as it is an often-missed requirement of some existing exemptions in UK data protection legislation. Several cases have now reached court on this, and it is clear that "necessary" will be a tough hurdle to jump in most cases. This means that consent is likely to be the most common option.

It is also worth noting that there is a carve-out to the list of Conditions, as EU Member States "may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."

The upshot is that when processing health data, the healthcare sector will have to implement their data processing operations in accordance with these conditions (or one of the other conditions). Healthcare organizations will as a result have to be more careful with the data and

more exact in knowing where it is being stored, how it is being processed and whether consent has been given.

CONSENT: ACTIVE REQUIREMENT

Consent has been fine-tuned under the GDPR and therein means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

This means that an active process will have to be put in place, which "could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data." It must also be demonstrated that consent has actually been provided. A clause of the GDPR permits consent to be valid where given prior to the full 25 May 2018 date of the application of the GDPR, as long as it is given in conformity with the GDPR.

One of the GDPR's health data conditions calls for "explicit consent," but the general definition makes no reference to the word "explicit." This has led to an on-going debate about whether there is a difference between "unambiguous" consent and "explicit" consent, and if so, what that difference might be. Far from being academic, this issue could affect the practical implementation of consent in products, services, websites, etc. However this ends up, explicit consent for healthcare purposes is very likely to always require the strongest forms of agreement, such as an opt-in tick-box or a declaratory statement.

The healthcare sector will also have to take a cutting-edge approach to obtaining consent. Consent will need to cover as many potential transfers of health data as possible, including international data transfers and cloud storage.

RIGHTS: MORE SARs AND OTHER CHALLENGES

New rights are being introduced under the GDPR, including the Right to Data Portability (allowing for data subjects to have their personal data sent back to them to transmit elsewhere more easily) and an extended Right to Be Forgotten (allowing data subjects to have their personal data erased without undue delay). While these are important, attention must be drawn to an existing right which has been subject to some significant tweaking, namely the Subject Access Right, or "SAR," a process where data subjects can exercise their right to gain access to their personal data. Under the GDPR, a SAR can be made free of charge and must be addressed quickly, i.e. within one month of receipt of the request (which may be extended for a maximum of two months when necessary, taking into account the complexity of the request and the number of requests).

The healthcare sector is no stranger to SARs, and their number has risen over the years; for example, the ICO estimated in June 2016 that 13% of UK residents had now made a SAR. This rise can be expected to continue once they are free, and SARs will become more costly and complicated for organizations to address, especially given the prevalence of email and cloud applications. In order to meet these challenges in a more timely and cost effective manner, the healthcare sector must revise its SAR policies and procedures accordingly.

DOES A DATA PROTECTION OFFICER NEED TO BE APPOINTED?

Under the GDPR, there is an obligation to appoint a data protection officer (DPO) in some circumstances. In the healthcare sector this will mostly be where, as a core activity (either as a controller or processor), health data of the three kinds mentioned above is processed on a large scale. The GDPR also allows for EU Member States to require DPOs to be appointed in circumstances other than those set out under the GDPR.

WILL SOME KIND OF PRIVACY IMPACT ASSESSMENT HAVE TO BE MADE?

Under the GDPR, what are now called "data protection impact assessments" (DPIAs) will be required when health data of the three kinds mentioned above is processed on a large scale. A DPIA is a type of risk assessment

of the impact of the anticipated processing activities on personal data. A data protection regulator will also have to be consulted prior to personal data being processed when an assessment "indicates that the processing would result in a high risk in the absence of measures taken by a data controller to mitigate the risk."

Our experience has shown us already that the DPIA process can be a useful way of reducing risks. For example, DPIAs may identify security risks which can be mitigated by specific processes, training or software. The healthcare sector will have to set up policies and procedures for undertaking DPIAs. While this may at first sight seem to be a compliance burden, the healthcare sector should consider that DPIAs enable them to obtain a better grasp on their data processes and reduce risk, and also help with security auditing.

ARE RAIDS POSSIBLE?

Under the GDPR, data protection regulators may "carry out investigations in the form of data protection audits." In

doing so, they may also "obtain access to any premises of the controller and processor, including to any data processing equipment and means," in line with the applicable procedural law. The healthcare sector has already been subject to health audits in the UK, which, combined with the fact that health trusts have a poor data security track record, heightens their vulnerability to being raided. In the 12 months prior to June 2016, the ICO reported the results of 38 audits, visits and reports in the healthcare sector, though it is not clear how many of those 38 were conducted on a voluntary basis.

MANDATORY SECURITY BREACH REPORTING

One of the most important changes under the GDPR is mandatory data breach reporting. Breaches must be reported to a data protection regulator within 72 hours, and those affected by the breach must also be informed. The healthcare sector will therefore have to put in place clear, practical and effective procedures that can be acted upon immediately—this should be at the top of its GDPR compliance checklist. It cannot be emphasized enough how important it will be to undertake training and fire drills.

Recent enforcement action by the ICO against the Alzheimer's Society serves as a case study for how things can go wrong and why training is so important. The charity had recruited volunteers to help dementia sufferers and their families or caregivers seek NHS funding. However, in their handling of the numerous cases, which involved drafting reports that included sensitive personal data, the volunteers used their own personal email addresses, stored data on their home computers unencrypted and failed to manage paper files correctly. No data protection training had been provided to the volunteers. These were the most recent in a line of data breaches, including the hacking of the charity's website, putting at risk some 300,000 email addresses. To compound matters, the ICO had previously audited the charity, which had not fully implemented ICO recommendations arising from the audit. Enforcement action included mandatory data protection training, policies and procedures to be brought fully to their staff's attention, and the use of encryption in portable and mobile devices. The ICO press release about the case can be found here: **https://ico.org.uk/about-the-ico/news-andevents/news-and-blogs/2016/01/ico-criticisesdisappointingattitude-of-dementia-charity/**

The healthcare sector should consider implementing preventive technical solutions to avoid breaches. Recent instances of the use of "ransomware," which include attacks against hospitals, highlight the need for those solutions.

GREATER PENALTIES

A key driver behind better compliance with the GDPR is the threat of increased enforcement supported by greater sanctions. For some infringements, a maximum fine of €20 million or 4% of the global annual turnover of a business (whichever is greater) can be imposed. The healthcare sector is no stranger to fines, and the highest fine to date in the UK is £325,000 imposed after computer hard drives containing patient personal data were stolen from the Brighton and Sussex University Hospitals NHS Trust. It is also important to highlight the following carve-out: EU Member States "may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State."

NEXT STEPS

The issues we have highlighted in this paper are the key ones concerning the healthcare sector, but are by no means exhaustive. To ensure compliance with all aspects of the GDPR and avoid possible future sanctions, the best way forward is for the healthcare sector to set aside appropriate resources and start preparing now. Some of the things to think about include:

1. **Thoroughly review vendor contracts. Vendors' help will be needed, especially in reporting security breaches quickly. Organizations should make sure that they have the contractual rights to insist on this, and they should make sure that they can hold their vendors accountable.**

2. **Prepare to update everything and make sure that your policies, procedures, documentation and records are ready for regulatory inspection.**

3. **Review all key practical aspects of the GDPR, including data retention and destruction.**

4. **Ensure that new aspects, such as explicit consent, the right to be forgotten and the right to not be subject to profiling, are all included in policies and procedures.**

5. **Put in place a data breach notification procedure, including detection and response capabilities, and consider purchasing special insurance.**

6. **Rehearse your data breach plans and make sure the organization can report on the consequences of a breach very quickly.**

7. **If applicable, appoint a data protection officer.**

8. **Put in place a data protection impact assessment policy/procedure.**

9. **Train staff on all the above.**

10. **Set up and undertake regular compliance reviews in order to identify and rectify issues.**

The GDPR go-live date may seem far away, but it's not. With proper planning, the GDPR doesn't have to be an insurmountable obstacle, but the time to start that planning process is now.

Learn More:
www.absolute.com/gdpr

Contact Sales:
1.877.600.2295
sales@absolute.com

AUTHORS

JONATHAN P. ARMSTRONG
CORDERY
LEXIS HOUSE
30 FARRINGDON STREET
LONDON EC4A 4HH
OFFICE: +44 (0)207 075 1784
JONATHAN.ARMSTRONG@CORDERYCOMPLIANCE.COM

Jonathan P. Armstrong is an experienced lawyer with a concentration in technology and compliance. He is based in London. His practice includes advising multinational companies on matters involving risk, compliance and technology across Europe. He has handled legal matters in more than 60 countries involving emerging technology, corporate governance, ethics code implementation, reputation, internal investigations, marketing, branding and global privacy policies. Jonathan has counseled a range of clients on breach prevention, mitigation and response.

Jonathan is one of three co-authors of the LexisNexis definitive work on technology law, "Managing Risk: Technology & Communications." He is a frequent broadcaster for the BBC and other channels and appeared on BBC News 24 as the studio guest on the Walport Review.

In addition to being a lawyer, Jonathan is a Fellow of The Chartered Institute of Marketing. He has spoken at conferences in the U.S., Canada, China, Brazil, Singapore, Vietnam and across Europe. Jonathan qualified as a lawyer in the UK in 1991 and has focused on technology, risk and governance matters for more than 20 years.

André Bywater is a commercial lawyer with a focus on regulatory compliance, processes and investigations.

His practice has engaged both the private and public sectors. He was Brussels-based for many years focusing on a multitude of EU issues during which time he worked across Europe and beyond. He has assisted and advised mainly European and US in-house counsel and other company personnel. Further, he has also addressed a variety of legal matters in the context of EU-funded projects building the expertise and capacity of government ministries and agencies in Central and Eastern. He brings to the practice a wide range of experience and skills. He qualified as a lawyer in the UK in 1993.

He is a Cambridge University graduate and a fluent French speaker with a reasonable command of Russian.

ANDRÉ BYWATER
CORDERY
LEXIS HOUSE
30 FARRINGDON STREET
LONDON EC4A 4HH
OFFICE: +44 (0)207 075 1788
ANDRE.BYWATER@CORDERYCOMPLIANCE.COM

ABOUT ABSOLUTE

Absolute is the leader in self-healing endpoint security with a fundamentally new approach that ensures uncompromised visibility and real-time remediation to stop breaches at the source. Our SaaS platform puts IT and security professionals in total command and control of devices, data and applications—whether they are on or off the network—to improve IT asset management, ensure compliance, protect data and reduce insider threats.

Our core technology advantage, Absolute Persistence, is embedded in over a billion popular devices, giving our platform and other endpoint controls the power to self-heal and withstand user errors or malicious attacks while returning to an original state of safety and efficacy. With this trusted two-way connection, our customers can see it all and secure it all with zero impact on users. More than 25,000 organizations and the world's leading device manufacturers including Acer, Dell, Fujitsu, HP, Lenovo, Samsung, and others rely upon Absolute's self-healing endpoint security solutions for the ultimate awareness and resilience. For more information, visit **www.absolute.com.**

/ABSOLUTE

Always There, Already There.

Only Absolute gives you the uncompromised visibility and real-time remediation to stop security breaches at the source. This is made possible by our Absolute Persistence self-healing technology, embedded in over a billion popular endpoint devices for the power to withstand user error or malicious attacks and return to an original state of safety and efficacy. No other technology can do this. For more information, visit **absolute.com.**

ABT-EMEA-Healthcare-EU-GDPR-WP-ENG-042717