Health data — regulatory trends and developments

The data protection team at McDermott Will & Emery advise EU and UK health and life sciences organisations to review their collection and processing of health data obligations, in light of the increasing number of GDPR enforcement actions

There is a common misconception that the term 'health data' in the GDPR and UK GDPR refers simply to medical records, but the definition is in fact much broader. All data concerning health, including significantly 'inference' data, fall within its scope. Inference data are that which alone or with other data sources would enable a third party to draw an inference about someone's health. This may include information about an individual's diet, their exercise levels, or attendance at a clinic.

Data relating to a person's health have long since been viewed as sensitive. Health data were protected under the previous Data Protection Directive (95/46/EC) and national law, including through the existence of professional obligations such as the doctor's responsibility to keep a patient's details confidential. As a result, the GDPR is not the only consideration when collecting and processing health data in the EU, EEA, and UK.

Conditions for collecting and processing health data

Consent has been a key feature in the provision of health services. Patients give informed consent for treatment, for example, and/or subjects give consent for their involvement in clinical research.

As a result, many organisations default to thinking that consent is the only legal basis under which they can handle health data, or that using consent is the 'gold-standard' to which they should aspire. While this is the case under many national, common laws and professional duties, and is still the case in the US, it is not the case under the GDPR. Under Article 9 of the GDPR, there are ten exceptions or conditions available for processing special category data permitting the collection and processing of health data. Consent is one of the conditions available. Other common conditions include that the data are being used for the provision of healthcare, in the interests of securing public health, or for research purposes.

Provision of healthcare: In order for this condition to be met, the processing must be necessary for one of the following:

- the purposes of preventive or occupational medicine;
- the assessment of the working capacity of the employee;
- making a medical diagnosis;
- the provision of health or social care, or treatment; or
- the management of health or social care systems and services.

In addition, the data must be processed by or under the responsibility of a professional who is subject to the obligation of professional secrecy or rules established by national competent bodies, or by someone subject to a legal obligation of secrecy or rules established by national competent bodies. The professional could therefore be a medical doctor or other healthcare professional who is part of the wider healthcare team.

Public health: The public health condition covers health data processing required by a legal or regulatory provision. Providing 'high standards of quality and safety of health care and of medicinal products or medical devices' may, for example, cover the processing by a medical device manufacturer of health data for the purposes of ensuring the proper functioning of the device, or for reporting adverse events to the health authorities.

Research purposes: The research condition permits health data to be processed for scientific research purposes if based on an EU or individual country's law, provided that the processing is proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The use of health data for research purposes is the most controversial of the GDPR's conditions and has been supplemented slightly differently at the country level because of its requirement for a basis in an EU or

individual country's law. This means that practice is not consistent among European countries and their Supervisory Authorities. Organisations that process health data for research purposes therefore need to be particularly mindful of local requirements.

In Germany, for example, research must be in the public interest and that public interest must outweigh the data subject's opposing data privacy rights. Interestingly, Supervisory Authorities are often reluctant to assume a public interest in a commercially driven research project. For example, if a medical device company conducts research to improve its products, this might not be considered as fulfilling the research condition, even if it could be argued that improvements to the product are in the interests of the device's users.

In France, where the research must also be justified by a public interest, the CNIL and the Health Data Hub in charge of construing the concept of public interest recognise that private research projects may be conducted in the public interest, as much as public research projects. The CNIL takes a very broad view on what qualifies as being in the public interest (e.g., improving care, public health or the healthcare system, research and knowledge enhancement, etc.).

In the UK, the Information Commissioner's Office ('ICO') has published draft guidance about research processing, and there are also proposals to change data protection legislation to allow for greater flexibility for research (see page 1 of this edition of *Privacy & Data Protection*). The ICO's approach is considered fairly flexible, although it is worth noting that the research condition will not be considered satisfied if the data processing is likely to cause individuals substantial damage or substantial distress, or if it is carried out for the purposes of taking measures or decisions about particular individuals, except in the case of approved medical research.

"The key to obtaining effective and legal consent is a well-drafted consent form. It should be written in clear language that does not overwhelm nor confuse the data subject, whilst also providing all the information necessary for the consent to be valid."

National laws on medical confidentiality

All EEA countries and the UK have national laws concerning medical confidentiality, which apply to the professionals handling information relating to their patients' medical histories.

The fundamental principle behind data protection law in the UK is that information shared by individuals with a professional should not be used or shared except as originally understood by the individual or with their subsequent consent, which can be expressed or implied. National Health Service legislation overrides confidentiality for certain approved research, but patients may choose to opt-out of this use to protect their privacy.

In Germany, doctors and other healthcare professionals are generally prohibited from sharing patient data with third parties without the patient's consent. Notably, a breach of professional secrecy obligations is not just sanctionable by the German medical association, the Bundesärztekammer, it is also a criminal offence. Doctors and healthcare professionals are, however, permitted to share health data with 'contributing persons', such as service providers who act in the interest of and on behalf of medical professionals, which includes IT service providers, or providers of practice management software.

France takes an extremely strict line on healthcare data. Medical confidentiality is an irrevocable duty imposed on healthcare professionals and even patients cannot consent to release them from their obligations if the law does not expressly permit it. Similarly, patients cannot grant consent for their healthcare data to be transferred to a third party. The main exception is in the context of secondary data processing for research, in which case the relevant organisation must first obtain an authorisation from the CNIL.

Consent

Although the Article 9 alternatives to consent outlined above are available, it is often the case that the conditions attached to them cannot be met and obtaining consent is the best option. In these situations, organisations need to understand what constitutes valid consent.

First and foremost, data subjects cannot be forced to give consent. They must be given free and ongoing choice in when and how their data are collected and processed, and they must actively choose to grant consent; they must 'opt-in' rather than 'opt-out'. Any request for consent must be prominent, independent from other terms and conditions, concise, and easy to understand.

Requests for consent must also be 'granular', meaning that they need to be very specific about how data will be used and for what purposes. They must also cover the name of the controller, i.e., the relevant legal entity that will process the data, and any other relevant controllers. When the processing has multiple purposes, consent must be given for each of them, which in practice means multiple opt-in check boxes and, because the data subject can remove consent for any one or more of these purposes at any time, there must be systems in place to manage every aspect of the consent.

The control given to data subjects over how and when their data are

(Continued on page 6)

(Continued from page 5)

used presents the biggest challenge inherent in relying on consent as a condition for health data processing. Under the GDPR, the data subject must be able to withdraw consent at any time, which forces the organisation to stop processing their personal data immediately. In the case of clinical trials, for example, if there is no other lawful basis and Article 9 condition for justifying the retention of the data for further processing, it must be deleted by the controller, which could have an impact on the reporting of serious adverse effects.

Consent form best practice

The key to obtaining effective and legal consent is a well-drafted consent form. It should be written in clear language that does not overwhelm nor confuse the data subject, whilst also providing all the information necessary for the consent to be valid.

As a minimum, the following points should be considered:

- it is easier to obtain, document, and manage consent if it is obtained electronically;
- because data subjects must actively opt-in, the use of pre-ticked boxes is not acceptable;
- even if there is limited space on the consent form, some context should be given. The data subject needs to know what is planned for their data. If necessary, a second page, additional text box or a web-link may be used, with a clear reference to it;
- the controller should be named. If health data will be shared with another legal entity, the latter should also be named along with the specific purposes for the data;
- an assessment should be made on whether or not additional, national medical confidentiality requirements apply. An additional check box or consent process may be needed to cover these;
- detailed information required under the GDPR, such as the rights of the data subject, may be referred to in the privacy policy. This can be one, all-encompassing document that covers all the controller's relevant data processing activities; and
- the form should refer directly to the policy, e.g., through a hyperlink, or by directing the subject to the controller's website.

Does anonymising data avoid the need for consent?

Data that have been anonymised are not subject to the GDPR because they do not constitute 'personal data'. There is, however, a fine line between anonymised and pseudonymised data, which is still personal data and therefore regulated under the GDPR. To a certain extent, the question hinges on whether or not an individual could be 'singled out' even if their name, address, and patient code have been removed from a data set. For example, singling out might be possible in small populations of patients who suffer from rare diseases, or when a patient has undergone a certain type of treatment in a specialised hospital.

In addition, identifiability exists on a spectrum, so it depends on how the data are processed or who holds them. For example, if a clinical trial company holds personal information about participants and uses an encryption method to anonymise those data, the data will not be anonymous within that organisation as it holds the decryption key. The same data may, however, be anonymous in the hands of a controller to whom that data are transferred, because the controller does not have the key.

For the CNIL, which takes a strict view of the EU case law, if the data are not anonymous in the hands of one organisation, the data will not be considered as anonymised even if held under an anonymous form by another organisation. Similarly, identifiability is subject to technological developments. If decryption techniques advance to the point where current safeguards are no longer effective, the data may no longer be anonymous.

Regulators have recognised that it may not be possible to achieve absolute anonymity forever; they state that what is important is that anonymisation is effective. It is worth noting, however, that 'effective' has multiple definitions. For the ICO, it means reducing identification risk down to a sufficiently remote level; for the CNIL, it means there must be zero chance of identification.

Regardless of whether an organisation has applied one of the GDPR's conditions to its data collection, or has opted for obtaining consent, unless health data are entirely anonymised, they should always be protected with the application of pseudonymisation techniques, encrypted servers, and additional access controls and safeguards.

Re-using health data

The re-use of health data can be challenging for a number of reasons.

The first challenge relates to how the data were initially obtained and under which condition. If, for example, the data were originally collected for research purposes, the secondary use is also for legitimate research purposes, and no national laws are triggered by the secondary use, it may be appropriate to re-use the data.

If, however, consent has been obtained for the primary purpose, the organisation will need to check whether or not the scope and content of the initial consent covers the secondary purpose. This is an excellent example of the impact of granular consent, and why consent should only be relied upon for the use of health data where absolutely necessary. It also shows the value of foresight when drafting a consent form.

The second challenge relates to data security. The GDPR requires additional safeguards when health data are used for secondary purposes, such as anonymisation or pseudonymisation to the extent compatible with the relevant research project.

The UK government and ICO have committed to changing the UK legal provisions on research in order to sim-

plify data protection compliance in the context of research. The ICO has issued draft guidance (www.pdpjournals.com/docs/888348) on using the Article 9 GDPR research condition in the UK. In the guidance, the ICO emphasises the purpose limitation exemption for consent in Article 5, which states that existing personal data can be re-used for research related purposes, as long as appropriate safeguards are in place, because this is considered to be 'compatible' data processing. The situation is different if consent was the original lawful basis for processing the data, in which case new consent is needed for each new use of the data.

The ICO also set out helpful guidance and criteria for what would be considered research in the public interest. For example, research activities that are peer reviewed, published, subject to ethics guidance or committee approval, compliant with rules on research, and are published are, according to the guidance, likely to be considered legitimate research.

In relation to re-using data obtained from another organisation, the ICO states that the recipient organisation is essentially collecting new data, not re-using or repurposing them. The recipient organisation cannot therefore rely on the original organisation's purpose and must instead identify its own lawful basis for processing. Data subjects should be informed that the data have been passed on and provided with the recipient organisation's privacy policies, unless doing so is impossible or involves disproportionate effort.

See the article on pages 12-15 of this edition of *Privacy & Data Protection* for an analysis of the identifiability provisions in the government's latest Data Protection and Digital Information Bill.

Enforcement trends

GDPR enforcement has been increasing across all sectors since 2019, in terms of both the number of fines and their size.

In terms of general trends, it appears that most fines have been imposed as a result of processing data with an insufficient legal basis, either because organisations did not apply for one, misinterpreted the legal basis, or obtained invalid consent because they were not familiar with the consent requirements. The second most common reason for fines was a lack of data security, which increases the risk of cyber attacks or third parties accessing the data. The third most common reason was organisations simply not complying with general data protection principles, e.g., by processing more data than actually needed for their purposes, or not deleting data when a specific project was concluded.

In the health sector, there appears to be an increasing number of enforcement actions relating to data security incidents. It is apparent that Supervisory Authorities across Europe are looking closely at the appropriateness of technical and organisational security measures such as pseudonymisation and anonymisation. Although Italy leads the field in imposing fines for GDPR violations, Germany and France are not far behind, suggesting that the Supervisory Authorities in all three countries have limited tolerance for health data being compromised. It is interesting to note that SAs are not exclusively targeting large pharmaceutical or medical technology companies. Fines are also being imposed on hospitals, doctors, and other players in the industry.

What the future holds: the European Health Data Space

The European Commission has published a draft European Health Data Space ('EHDS') Regulation (www.pdpjournals.com/docs/888349) with the aim of creating a common space where researchers, innovators and policy makers can use electronic health data in a trusted and secure way, preserving privacy and the rights of data subjects to control their data. The draft EHDS Regulation addresses the challenge of establishing such a space by promoting the digital transformation of the use and access to health data in healthcare (primary use), and regulating electronic health records ('EHR'); and accelerating the re-use (secondary use) of individuals' health data.

The draft Regulation also builds on the requirements that have been imposed on software through the Medical Devices Regulation and the proposed Artificial Intelligence ('AI') Act. In order to avoid any regulatory gap, where manufacturers of medical devices (which need to be certified under the Medical Devices Regulation) and high-risk AI systems (which should be subject to risk management, security requirements, and certification under the draft AI Act) will need to comply with interoperability requirements, to the extent they claim interoperability with EHR systems.

United States perspective

Unlike the UK and the EEA, the US has multiple federal and state privacy laws specifically focused on individual sectors, including the health sector. Some of the laws regulate types of organisations within specific sectors, such as mental health facilities or subcategories of health data, such as genetic test or HIV test results. As a result, privacy protections often depend not only on whether the data are health-related, but also on who holds the data. For example, if a consumer uploads personal health data to a mobile app, the app developer may be unregulated in most states (beyond basic federal law expectations to comply with privacy promises in a published privacy policy), but the same data held by a hospital may be protected by multiple laws.

The primary law regulating personal health data in the US on the federal level is the Health Insurance Portability and Accountability Act of 1996 ('HIPAA'). HIPAA regulates certain health care providers, governmental and private health plans, and healthcare clearinghouses, which are intermediaries between providers and plans.

HIPAA defines 'protected health information', with certain exceptions, as information that meets the following two criteria:

- the information must relate either

(Continued on page 8)

(Continued from page 7)

to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

- the information must also identify an individual, or there is a reasonable basis to believe the information can be used to identify the individual.

In the US, consent is generally seen as the gold standard for processing data.

HIPAA does not require a legal basis for the use of de-identified data and it requires re-identification risk to be reduced to a "very small," but not zero, level of risk. HIPAA's willingness to allow data sets that involve only a very small residual risk of re-identification to be considered de-identified and outside of HIPAA privacy requirements reflects the HIPAA Privacy Rule's policy goal of reasonably balancing the competing goals of data utility and privacy.

Two de-identification methods are permitted under HIPAA: 'safe harbor' and expert determination.

Safe harbor: Under the safe harbor method, a HIPAA-regulated entity must remove 18 identifiers, which include direct identifiers (e.g., name and email address) and indirect identifiers (e.g., birth dates and other dates more specific than year).

Expert determination: This method is comparable to the singling-out approach under the GDPR. Health information is considered de-identified under the expert determination method if someone with expertise in generally accepted methods for rendering information not individually identifiable determines that the risk the information could be used to identify an individual is very small, and documents the methods and results used to make this determination.

Key takeaways

'Data concerning health' covers a lot more than medical records. Policies and processing records should accurately capture all health data, including inference data.

Most EEA countries and the UK have national laws that supplement the GDPR. Consent is not the only legal basis for collecting, storing and using health data — other options are available — but organisations need to be aware that "insufficient legal basis for data processing" is a common type of GDPR violation.

If used, health data consents must be granular, specific, and transparent, and they must break down all the purposes for which the data are being processed. Consent must be granted on an 'opt-in' basis and not as a result of a pre-filled tick box. Health data may be re-used for genuine scientific research purposes, provided the processing is compatible with the original use, appropriate safeguards are in place, and any separate national law conditions are satisfied.

Privacy policies and transparency notices must be clear about the basis on which health data are processed. Organisations should proceed carefully and consider any re-identification risks when relying on anonymisation to process data. They should also document any re-identification risk assessment and periodically review risk assessments in light of developments in publicly available data and evolving risk environment. Technical measures, such as evolving encryption standards, should also be reviewed periodically.

Sharon Lamb
Dr Deniz Tschammler
Daniel F Gottlieb
Lorraine Maisnier-Boché and
Pilar Arzuaga
McDermott Will & Emery
slamb@mwe.com
dtschammler@mwe.com
dgottlieb@mwe.com
lmaisnierboche@mwe.com
parzuaga@mwe.com