Enable data-driven healthcare & research for citizen benefit while protecting patient privacy

Call to Action

This Call to Action was created for use by Member State representatives, DPAs, health leaders and is intended to be aligned to the principles, conclusions and direction of “Health in the Digital Society, Digital Society for Health” in Tallinn, Estonia October 16-18, 2017.

The EU’s General Data Protection Regulation (GDPR) represents an important step forward for EU residents and the protection of their personal data. The Regulation clarifies data subjects’ rights, brings more organisations under its remit, and imposes significant sanctions for noncompliance with its terms. Health data, one of the more sensitive types of personal data, is especially called out in the new data protection rules.

When GDPR was drawn up, one of the overall goals was to establish harmonized data protection rules across the EU. On some issues, the final text however gives EU member states some flexibility to adapt the rules to their national interests. One area where such flexibility is foreseen relates to the use of health data. We believe it is important that Member State policymakers use this flexibility in order to enable data-driven healthcare and boost research ecosystems. Decisions taken now will govern life-changing moments for patients for years – even decades – to come:

100 patients in an EU country are treated for a particular type of cancer. Their data is kept in official records.

In the next few years, 40% move out of this EU country and become potentially unreachable.

Olivia presents with a rare variant of the same disease.

If this EU country requires specific consent for all research & treatment uses of data:

40% of the data may be unusable unless all identifying (but useful) information is removed. The result of the study may be statistically biased.

If this EU country does not require consent to justified use of data for research and treatment:

100% of the data is usable, and leads to a breakthrough.

Olivia is safely treated.

Conducting a new study of the historical data holds the key to her getting the best possible treatment.

The result of the study may be statistically biased.
We encourage Member States to exercise the power given to them under the GDPR to allow the processing of health data for healthcare, scientific or statistical research purposes, or reasons of substantial public interest, even in scenarios where consent is not feasible or appropriate.

1. Take Advantage of the Flexibilities in the GDPR to Enable a Wide Range of Beneficial Uses of Health Data.

Under the GDPR, organisations must have a legal ground to process personal data. When it comes to health data, the default ground is generally consent. In the medical context, however, the GDPR gives Member States the ability to permit processing of health data without consent in some circumstances. This includes instances where processing is necessary for medical reasons (including treatment, diagnosis, preventive medicine, and workplace health), and the management of health or social care systems and services – so-called “primary” or “direct” processing scenarios. The GDPR also allows for processing of health data without consent where it is necessary for scientific research purposes, or for public interest in public health – known as “secondary processing”.

GDPR foresees that to benefit from these flexibilities for the processing of health data, EU Member States or the EU must pass legislation which permits and enables these uses. Allowing for these uses can make sense. In oncology, for example, cancer registries have enabled numerous advances in cancer treatment and prevention. If such registries were required to ask every patient for consent, participation rates would often be lower than required, and therefore lead to statistically biased results. Moreover, for registries already holding several decades’ worth of data, it would likely be impossible to retroactively contact each individual data contributor to seek consent for each new research project.

This issue is one facing public and private researchers alike. A great deal of valuable healthcare and research collaborations occur outside the public sector; for instance, in consortia mixing private and public entities such as universities and hospital research units.

The “positive discretion” under GDPR presents an opportunity for EU Member States to allow for the best possible health care data use with an appropriate balancing of patient privacy rights. EU Member States, which do not use this opportunity could disadvantage patients, domestic researchers and healthcare providers, in the development of potentially life-saving and cost-saving advances in research and care.
2. Researchers need to be Confident they can Process Health Data Lawfully

Besides implementing legislation, EU Member States also have the opportunity to provide supportive guidance and interpretation of key terminology in GDPR. Constructive interpretations of terminology such as "scientific research" and "adequate safeguards" by EU Member States can stimulate research and enable public health officials, healthcare providers and patients to benefit from advances that will improve health outcomes and reduce the cost of care.

GDPR allows of the use of health data for a range of research purposes – including "scientific research" – without specific consent of the data subject where national or EU law so allows. But to be lawful, the processing must be "subject to appropriate safeguards." Clear guidance around what constitutes "scientific research" and what types of "safeguards" are "appropriate" will help empower data driven research.

The GDPR provides some guidance for the interpretation. For example, it states "scientific research" is to be broadly construed and can include technological development and demonstration, as well as privately-funded research. We encourage wider affirmation of the basic principle: it is essential that these principles and positions be reflected in guidance, codes of conduct and public discourse, given their essential practical role in day-to-day implementation of the GDPR.

In terms of "appropriate safeguards," the GDPR mentions pseudonymisation and data minimisation as possibilities, but otherwise does not specify what else would satisfy the requirement. To provide certainty and enable healthcare providers and researchers to rely on the ground with confidence, regulators should identify other examples of "appropriate safeguards" that will be deemed acceptable. In doing so, they should draw on the substantial research ethics and data guardianship expertise that researchers in both the private and public sector have accumulated over numerous years.

In order to ensure compatibility with other countries and maintain the ability to participate in global research initiatives, EU member states should also aim to ensure that their interpretations and guidance remain open-ended and flexible.
3. Refrain from Imposing Additional Limitations on Health Data

We encourage Member States to be cautious in maintaining or introducing further conditions, including limitations, on the processing of health data, particularly as it relates to processing of health data for primary use. Imposing additional restrictions and requirements on such processing may have the unintended consequence of undermining the delivery of care across Member State borders and hindering development and use of innovative care tools.

The EU's primary purpose in replacing the 1995 Data Protection Directive with an EU-wide Regulation was to unify the data protection regimes of Member States, in order to create a more consistent regulatory environment and a single European Research Area. Member States should of course keep that goal of unification in mind as much as possible.

Despite that goal, the GDPR does allow Member States some “negative” discretion to adopt even stricter rules in relation to health data. However, there are important legal limits to how much stricter those can be. For example, the GDPR is clear that local data protection rules must not prevent healthcare providers from processing or storing health data in other EU Member States.

For both legal and ethical reasons, Member States should refrain where possible from exercising their “negative” discretion. Maintaining or adopting new limits on processing of health data would impede the roll-out of many new, emerging and future technologies and studies that promise to deliver better quality, more affordable care.

At the very least, Member States should avoid introducing any further rules that would interfere with a healthcare provider’s selection of tools or technology for use in treatment of individual patients, including diagnosis, billing or other ‘primary’ uses of the patient’s data. Requiring providers to seek consent to use particular types of technology for purposes such as diagnosis, billing or other primary uses of patient data—such as analysing data in the cloud to help inform a diagnosis—could impede the provision of high quality care for individuals.

Requirements that health data be stored or processed in a particular location (e.g., hospital premises, or the Member State in which care is being provided) have a similarly detrimental effect on care. They are also at odds with the Union’s goals in this area, including free movement of data, ensuring health care for a mobile workforce, and an integrated single market for technology and services.

In addition to an adverse impact on direct care, policymakers should also be acutely conscious of the adverse effect that localisation requirements have on scientific research. They could in effect ban otherwise legitimate projects or push up compliance costs. They will also disrupt Europe’s ambitions to build a common research area, by subjecting multi-country research efforts to a dizzying patchwork of local rules.
4. Provide Guidance Related to Appropriate Security Measures and Codes of Conduct

EU Member States should build on the expertise of the private and public healthcare industry and its partners for security controls and safeguards for sensitive health data. The expertise will help EU Member States to adopt security policies and supporting codes of conduct which align with global security standards and best practices.

GDPR requires that parties processing personal data must implement security practices that are appropriate to the level of risk. In order to determine the level of security for health data, a number of criteria need to be considered, including state of the art security tools, costs of implementation, and the nature, scope, context and purposes of the data processing. Recognising that the state of the art security and the cyber risk landscape evolve rapidly, GDPR does not mandate specific security practices to be followed.

As Member States and organisations contemplate what security practices are optimal, they should look to global best practice standards and default to globally harmonized solutions.

In the health sector, regulatory and industry practices in many Member States are increasingly aligned to established global standards. For example, in the Netherlands, the NEN-7510 standard serves as the security baseline for healthcare organisations handling patient health data and is based on the established ISO/IEC 27001 international security standard. Similarly, a new framework being rolled out in France to govern hosting of health data relies heavily on ISO/IEC 27001 and other ISO standards. Industry has already been using ISO/IEC 27001 for many years and can therefore provide expertise to Member States aligning to these global standards.

The GDPR also encourages the use of data security codes of conduct and sets out a legal framework for their official recognition. Codes of conducts have the benefit of being adaptable to technological and legal developments and therefore tend to be more future proof than laws. Member States should seize upon that opportunity to leverage the experience and thought leadership of health and technology sector associations in establishing the appropriate security measures for the processing of health data. Ideally, Member States can help industry to enshrine these practices in easily-updated codes of conduct, rather than laws or government policies which may be more challenging to keep updated.
1. Take advantage of the flexibilities built into GDPR to allow for wide range of beneficial uses of health data. This includes a full and flexible implementation of the grounds in Article 9(2) of the GDPR.

2. Ensure legal clarity for the research community on the use of health data by providing clear definitions for key terminology. It is of particular importance to define broadly the concept of “scientific research” as set out in GDPR Recital 159, which ensures that health data can be processed for public research, private research and technological development.

3. Through dialogue with public health authorities, members of the research community, patient stakeholder groups and members of the healthcare and medical technology sectors, clarify the additional types of “appropriate safeguards” that can be put in place for processing health data for research purposes under GDPR Article 89(1).

4. Resist maintaining or imposing local limitations on use of health data under GDPR Article 9(4), particularly where direct care for patients may be affected – for instance, additional local conditions on the use of cloud computing resources by clinicians – so that patients can enjoy the full benefit of cross-border healthcare services and international research collaboration.

5. Base any local data security requirements on global security standards and best practices and leverage the expertise of health and industry associations in efforts to define appropriate security measures, including through support for codes of conduct that embody those requirements.