Proposal of the European Commission for a Regulation of the European Parliament and of the Council relating to General Data Protection - 2012/0011 (COD)

HOPE position

HOPE is the acronym of the European Hospital and Healthcare Federation, an international non-profit organisation, created in 1966. HOPE includes national associations of public and private hospitals and of owners of hospitals. Today HOPE is made up of organisations coming from 27 Member States of the European Union, as well as from Switzerland and Serbia as observer members.

HOPE welcomes the Commission's effort to further harmonise data protection requirements in the European Union. HOPE also welcomes the provisions to support healthcare and health research. However, some areas must be improved to facilitate improvements in care delivery, continuous medical innovation and, to support medical research for the benefits of society. A considerable number of provisions will restrict the availability of health data, delay innovation, create legal uncertainty and increase compliance costs if they remain unchanged.

Access

It will be challenging for healthcare organisations to meet the timeline stipulated in article 12 to respond to access requests. Not only healthcare organisations receive a large number of requests but a significant proportion of health records are not yet available electronically.

Healthcare organisations are working to input all data retrospectively but this is a huge undertaking as it requires inputting data for the entire duration of the individual health record of every single data subject within their system as well as from across other systems. The healthcare environment has a multi-contributory records environment.

There is also a need to ensure that any data passed on to the data subject does not inadvertently betray the privacy of third parties who may be mentioned within the record. For this reason, the record may have to be adapted before it is shared with the data subject. More time is required to do this.

Finally, it is unrealistic in a health context to specify how long data may be stored for beyond 'as long as may be deemed necessary in order to guarantee the appropriate delivery of healthcare to the data subject'.

Right to be forgotten

Article 17 introduces the right to be forgotten but data subjects have no interest of the permanent erasure of data pertaining to health, particularly where such data is relevant to the effective and appropriate delivery of healthcare.

Deleting data from electronic health records may run counter to patient safety: healthcare providers will not have access to life-saving information on the patient when establishing a diagnosis: allergies, ongoing treatments, specific conditions (e.g. diabetes), blood type, medical history, etc.

Statistical analyses might be "depowered", particularly in the case of orphan diseases or conditions with difficult inclusion and exclusion criteria, such as paediatrics.

Healthcare providers might object to the deletion of data for liability issues: in case of investigation clinicians need to refer to the patient record to justify their decisions and treatment delivered.

Article 17.3 (b) suggests that the right to be forgotten does not apply in the healthcare context where there is a 'public interest'. The concept of 'Public interest' is not clear in the healthcare context.

For clarity, HOPE suggests that the right to be forgotten should not apply where the retention of personal data is necessary for health purposes in accordance with Article 81.

Data Portability

With article 18 data subjects would be getting the right to obtain from the controller a copy of data undergoing processing. The regulation should introduce the need for a way of verifying the authenticity of health information provided by the data subject, when such information is to be used to receive healthcare or for some kind of formal assessment of the individual.

Processing activities

Healthcare providers already retain detailed documentation of their processing activities. Article 28 is not clear in terms of whether every individual processing operation should contain the information detailed in Article 28.2, or whether this is a more general stipulation. For example, an healthcare organisation may as a general rule, state the information listed under Article 28.2. However it will not maintain individual records for every individual patient or episode of care. This general information will be made publicly available and the list (points a – h) may be revised annually.

Clarification is needed when referring to 'all processing operations' under Article 28.1. Article 28.4 exempts an enterprise or organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities. The number of employees an organisation has or the fact that the data processing is not the organisation's main activity does not, in a healthcare context, render that data any less sensitive. There should not be a two-tier system of data privacy based on the number of employees an organisation contains.

It is not clear precisely what 'an activity ancillary to its main activities' may mean in the healthcare context. Considering that the main activity of healthcare organisations is to provide care, will the processing of data be considered core to that or ancillary? This is an important point given that many healthcare providers are considered independent or belong to organisations employing fewer than 250 employees.

Impact assessment

Requirements for data protection impact assessment introduce unnecessary bureaucratic complexity. Article 33 requires that the processing of data concerning health is subject to the data protection impact assessment requirement. The criteria for impact assessments are not yet clear as the Commission may clarify them by delegated act under Article 33 (6). While clarity is crucial to understanding under precisely what circumstances assessments are required, it is equally important that the processes used by varying types or organizations (healthcare provider organizations, medical research organisations, eHealth service providers, etc.) are not constrained by prescriptive specifications under delegated acts. Given that processing activities are often different, impact assessments should not be "one-size-fits-all," rather they should be relative to the scope of processing, volume and type of data, and organizational aspects of those entities performing the assessments. Moreover, the data protection impact assessments will cause serious financial and administrative difficulties to small and medium sized medical practices.

In addition, while Article 34 provides for a prohibition to start the data processing before approval by the supervisory authority, it does not specify timelines for processing of requests by national authorities. Legal certainty as to when a decision can be expected on the adequacy of impact assessment is crucial for stakeholders.

HOPE recommends that a data protection assessment should be permitted to cover similar processing activities and activities, which present similar privacy risks. Healthcare organisations should be able to construct their own assessment, based on their specific type of organisation, legal requirements, contractual obligations, and, where appropriate, internal policies. Impact assessments should not constitute unbearable administrative and financial burden to small and medium sized medical practices. Prior consultation should not be needed when processing is based on consent or contract. Where approval is required, a clear time line for the approval should be clarified prior to effective dates.

Research

Anonymised, and pseudonymised or key–coded data are used by the health sector to conduct medical research, monitor the efficiency of treatments, monitor disease trends, support public health policies, etc. HOPE recommends the Regulation is amended so that it is clear how the scope of the Regulation relates to the different types of data used by the healthcare sector and to ensure that the processing of these different types of data are regulated proportionately. One route to achieve this clarity and proportionality is to clearly exclude from the scope of the Regulation data that do not relate directly to a data subject in the context of health or research.