General Data Protection Regulation
NHS European Office Position Paper

Impact on the healthcare sector

The health sector is responsible for controlling and processing a significant amount of personal data, not just in terms of the provision of care, but also in terms of research and employment. While the European Commission has gone some way to recognise the special nature of personal data processing in each of these areas, further work is required to ensure that this necessary and timely revision of the existing Data Protection Directive strikes the right balance between data privacy and the efficient delivery of healthcare services. The following areas require further attention:

- **Data Portability**

Data Portability is important particularly in view of the Cross Border Care Directive. However in order to guarantee 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, the health information provided should contain a form of verification to guarantee its accuracy. For example if an employer wishes to see a copy of an individual’s health record, they should be assured that no significant data has been removed from that record which may impede their ability to perform the functions of the role.

Alternatively in a healthcare context, if the data subject has a contagious condition such as hepatitis or TB, it should not be possible for the data subject to actively remove this information from their health data prior to sending it on to the healthcare provider if this information is relevant to their treatment. Serious health complications could arise if the data subject were able to adapt their health information prior to treatment. The health data should therefore be ‘locked’ or guaranteed via some form of verification model from the sending clinician to the recipient.

Article 18 also refers to ‘an automated processing system’. What does the Commission intend this to mean? Anything non-paper or something more sophisticated? This is important to the healthcare environment as much of our data is not yet stored electronically. The intended definition of this term may affect our ability to transmit data into another automated processing system.

- **Right to be Forgotten / Rectification**

The permanent erasure of data pertaining to health particularly where such data is relevant to the effective and appropriate delivery of healthcare, is not in the best interests of the data subject. Article 17.3 (b) suggests that the right to be forgotten does not apply in the healthcare context where there is a ‘public interest’. What does ‘public interest’ mean here? If it is to be interpreted as a general interest to the public at large, i.e. as a collective whole, then this is not enough. There is also a personal interest to every individual member of the public (citizen), which should be considered at this point. For clarity it would be better to suggest 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.
In the same way with regards rectification, it is important in a healthcare context that medical hypothesis and speculation can be retained within an individual’s health record as this may prove crucial to the appropriate delivery of healthcare to the data subject at a later date.

- **Access**

The NHS is wholly in support of measures to improve and enhance patient access to their health records. From a practical perspective however, it will be challenging to meet the timeline stipulated to respond to access requests. This is because a significant proportion of health records are not yet available electronically and is also due to the large number of requests individual healthcare providers receive. Health providers 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’.

- **Documentation**

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 a hospital 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.

What does the Commission mean when referring to ‘all processing operations’ under Article 28.1? The NHS would suggest clarity at this point to avoid an unintentionally over-burdensome Regulation, for example, removal of the word ‘all’.

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.

At this stage it is not clear precisely what ‘an activity ancillary to its main activities’ mean in the healthcare context. Our main activity is to provide care, is the processing of data to be considered core to that or ancillary? This is an important point given that many healthcare providers are considered

---

1 Currently in the UK the NHS is required to respond in 40 days, but this follows a formal procedure and payment.
2 Guys and St Thomas’ Hospital in London receives on average 750 data requests per month.
independent or belong to organisations employing fewer than 250 employees, for example; GP surgeries.

- **Consent**

The NHS European Office supports the Commission’s approach to consent where healthcare and research is concerned. We would however welcome clarity within the text to explicitly state that where personal data concerning health is processed according to the terms and conditions of Article 81, explicit consent is not required.

- **Research**

In order to preserve conditions necessary to promote research, anonymous and pseudonymised data should not be included within the scope of the Regulation. The process of anonymisation should also be excluded from the scope.

- **Private body, Public service?**

The proposed text allows public authorities (and bodies) to be exempt from certain requirements in Articles 33, 44 and 75. We welcome these exemptions on the basis that it is not the Commission’s intention to interfere with public authorities in the exercise of their public powers. However, it is not clear whether the exemption would apply to private providers contracted by a public authority to carry out a public service. It should be the nature of the service that defines how the Regulation applies, rather than the type of body carrying out the activity. (A GP for example, is contracted to carry out a public service, but GPs are not considered public authorities or bodies).