Revision of the EU Directive on Data Protection:

Key issues paper & recommendations to the Ministry of Justice

We welcome a revision of the existing EU data protection legislation in order to take into account advances in technologies and to harmonise data privacy standards across Europe. We are mindful that the proposal for a General Data Protection Regulation will have a significant impact on the health sector and is of critical importance to the NHS. Changes in the EU legislation will dictate data management processes in the NHS, at a time when the NHS landscape is experiencing dramatic change and large scale data programmes are being developed to support better care for patients.

This paper, which has been co-ordinated by the NHS European Office, defines the joint position and recommendations from the Department of Health, NHS England, Public Health England and the Health and Social Care Information Centre on issues of critical importance.

It should be noted that the NHS European Office has worked closely with a number of UK stakeholders on the use of personal data for research purposes, and is signatory to the position of non-commercial research organisations and academics entitled ‘Protecting health and scientific research in the Data Protection Regulation’. This remains our position on the subject of research, and this is why we have not covered this area in this paper.

- **Scope**

**Pseudonymisation**

We believe that it is preferential to maintain the European Commission’s (EC) original proposed text (COM(2012)0011), which leaves pseudonymised data or pseudonymisation out of the definitions in Article 4. This is because it is very difficult to create a definition that works across all sectors.

**Codes of conduct**

In recital 23 of the EC’s proposal we would welcome a reference to guidance or codes of conduct as instruments for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible. This provision is included in recital 26 of the current European Data Protection Directive (95/46/EC) and both the ICO anonymisation code of practice and the HSCIC guide to confidentiality in health and social care have become important practical guides for the UK context.

In light of this, it could also be appropriate to reference codes of conduct on pseudonymisation and anonymisation in Article 38 of the current proposal (COM(2012)0011).

---

1 The Department of Health, NHS England and the Health and Social Care Information Centre were not signatories to that paper.
Measured, risk based approach

We also would strongly support the EC’s original definition of ‘data subject’. From our perspective, it is crucial to ensure that the final text maintains the wording “by means reasonably likely to be used”. The European Parliament (EP) has proposed deleting this phrase from the definition. We think this text is extremely important as it recognises the necessity to take into account the context when defining whether data are at risk of being identifiable. This wording ensures that anonymisation does not have to be completely risk free. It is clear that the risk of identification must be remote (particularly for the special categories of data the NHS processes), but 100% anonymisation is not the legal test.

Recommendation 1:

<table>
<thead>
<tr>
<th>Maintain the European Commission’s original definition of ‘data subject’ in Article 4 of its proposal (COM(2012)0011), notably the phrase : “by means reasonably likely to be used”.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refrain from adding a definition of pseudonymisation to Article 4 of the Commission’s proposal.</td>
</tr>
<tr>
<td>Reference the benefits of Member State (or other) codes of conduct on anonymisation or pseudonymisation in recital 23 and/or Article 38 of the current proposal (COM(2012)0011).</td>
</tr>
</tbody>
</table>

- Free access to data (Article 12)

Article 12.4 (COM(2012)0011) states that information provided to the data subject should be free of charge, ‘unless where requests are manifestly excessive, in particular because of their repetitive character’. Dame Fiona Caldicott’s Information Governance Review addressed concerns about patients’ frustration in accessing their medical records. The recommendation is that people should have fullest possible access to all the electronic care records about them, across the health a social care system, without charge. This is clearly an important patient right and for electronic records it is certainly the strategic direction that UK health and social services organisations are taking. However, currently Department of Health guidance issued to the NHS, allows charges to be made - a maximum charge of £10 for electronic records, and a maximum of £50 for records held in another format has been imposed. Guidance is very clear that no profit should be made from the activity. In the case of a service like the NHS, the customer/patient always has to pay for this service either directly or indirectly. A medium sized district Trust can receive approximately 50 requests every week. While the NHS in general, and many Trusts are moving to electronic records, in most cases, a significant part of a data subject’s health record remains mostly paper-based, and rather voluminous. It is time consuming and costly to go through the archives to find a complete record and for this reason many Trusts still charge the maximum £50 charge, in order to cover costs. If that information had to be provided free of charge, it will take funds from other services in order to cover costs. As an example, when a medium sized NHS Board in Scotland conducted an audit of access to health records requests a few years ago, they calculated the real cost to the NHS Board was approximately £400,000 per year². While there is a strategic decision to aim for a

---

² These costs take into account, finding the records, a middle grade health records person going through the record to ensure that the request is fully complied with and the time lost to the NHS, whilst the individual is undertaking this activity, any redaction and the administrative costs such as photocopying and sending the records by either courier or recorded delivery.
paperless NHS, and for medical records held electronically to be provided to a patient free of charge, NHS organisations would greatly appreciate the flexibility to continue to charge, particularly for paper records, in order to reduce the cost and redirection of funds from other core services.

Recommendation 2:

Amend Article 12.4 (COM(2012)0011) to: ‘The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, or where requests are for data from a complex paper record held as part of a task carried out as a legal/ public duty, such as a health record, the controller may charge a fee for providing the information....’

- The right to be forgotten and to erasure of personal data (Article 17) and the right to object (Article 19).

It goes against good medical practice and current guidance in the UK to delete any information from medical records, unless ordered by a court. Even if the information in the record is corrected, a note is placed on the record and the audit trail is kept. The exemption given to controllers from the necessity to erase data without delay in a case where the data subject objects to the processing is given under Article 19.3 of the EC proposal (COM(2012)0011). However, the exemption for health purposes (19.3b) provides legal uncertainty because it only defines public health purposes under the exemption, which would not include the individual health care purposes required for keeping a complete medical record for each data subject. A simple addition to the text would solve any issues with legal uncertainty.

Recommendation 3:

Amend Article 19.3 (b) (COM(2012)0011) to: ‘for health purposes or for reasons of public interest in the area of public health in accordance with Article 81’

Chapter IV

This Chapter, which details the obligations of data controllers and processors, takes the principle of a ‘one size fits all’ approach, which is difficult to apply across every sector, and across each EU Member State. While we welcome a level of harmonisation across sectors, we believe this chapter will be difficult to apply and in parts becomes too prescriptive. We are particularly concerned about two areas of the chapter:

- Documentation (Article 28)

We are concerned about the necessity for the data controller and processor to maintain documentation of all processing operations under its responsibility. The word ‘all’ is infinite and is therefore concerning from a healthcare perspective, where many data processing activities take place in each episode of care. A strict and legalistic interpretation of this text could have great administrative and cost implications for the NHS and healthcare providers in the UK, while achieving very little in terms of data protection for the patient.
Recommendation 4:

Amend Article 28.1 (COM(2012)0011) to: ‘Each controller and processor and, if any, the controller’s representative, shall maintain appropriate documentation of all processing operations under its responsibility’.

- **Data Protection Officer (Articles 35-37)**

As the detailed Articles on this post (Designation of the DPO, Position of the DPO and Tasks of the DPO) are too prescriptive and disproportionate, we currently support the Council’s draft proposal to make this a voluntary position. At the very least the provisions in Articles 35-37 would be best placed in implementing legislation, and not in the text of the Regulation itself.

Recommendation 5:

Amend Article 35 (COM(2012)0011) to: the controller and processor shall may designate a data protection officer in any case where...

- **Processing of personal data for health purposes (Art 81)**

Article 81 of the EC’s proposal (COM(2012)0011) gives exemption for explicit consent for the ‘processing of personal data concerning health’. We support the Council’s discussions on broadening the scope of the title of this article as this could better support UK practice, which has a shared health and social care data management system, particularly for those involved in the direct care of the patient.

Aside from the title of the Article, we broadly support the EC’s original proposed text on Article 81 (COM(2012)0011), as opposed to the changes made to this Article by the European Parliament, which are particularly problematic. We have however one comment on the original Commission text. Paragraph 81.1(a) states that data must be processed by a ‘health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies’. While everyone processing personal data will have a contractual obligation of confidentiality, we are concerned that the broad scope of individuals involved in the direct care team may not fit entirely into the definitions of professionals who can process personal information given in 81.1(a). The text seems to suggest the person processing the data should come from a regulated profession. This may be problematic for the NHS as we are aiming towards a more integrated health and social care system. The HSCIC guide to confidentiality states that ‘members of a care team should share confidential information when it is needed for the safe and effective care of an individual’. Safe and effective care is dependent upon relevant confidential information being shared amongst all those involved in caring for an individual. There is a wide team, including social workers, doctors, nurses, laboratory staff, social care staff, those that provide specialised care and the administrative staff who support care provision who may have access to personal data as a member of the direct care team, not all of whom have regulatory bodies.
Recommendation 6:

Amend 81.a) (COM(2012)0011) to: ‘...health professional subject to the obligation of professional secrecy or another person also subject to an \textit{equivalent} obligation of confidentiality under Member State law or rules established by national competent bodies’

Contact: Sarah Collen-Godman, NHS European Office
Tel: +32 2 227 6441
Sarah.godman@nhsconfed.org