Information Commissioner's Office
Swyddfa'r Comisiynydd Gwybodaeth

Upholding information rights Cynnal hawliau gwybodaeth

2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH
Ail Lawr, Tŷ Churchill, Ffordd Churchill, Caerdydd, CF10 2HH
T. 029 2067 8400 F. 029 2067 8399 E. wales@ico.org.uk
www.ico.org.uk

Response to Consultation: Records Management Code of Practice for Health and Social Care 2016

Background to the Information Commissioner's Office

The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations. She upholds information rights in the public interest, promotes openness by public bodies and data privacy for individuals. She does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken. The opportunity to respond to this consultation is therefore welcomed but comments will only be made in respect of relevant to the scope of her responsibilities.

A) General Data Protection Regulation

In May 2018 the Data Protection Act 1998 (DPA) will be replaced by the General Data Protection Regulation (GDPR). Many areas of the proposed Records Management Code either draw on or refer directly to the DPA, and it would seem beneficial to review the Code of Practice and associated Letter before publication in Wales to ensure that it will be compliant with GDPR, and that it cross references GDPR where relevant. In any event, a GDPR-compliant version of the Code must be produced for adoption from May 2018. Importantly, the current 8 principles of data protection which underpin much of the IGA document and are quoted on p7 will change under GDPR. There will be changes to the rights of the individual, and the addition of a new principle of accountability which requires all data controllers to be able to demonstrate their compliance with data protection.

Examples of such changes include:

- the DPA definition of a "health record" is cited on page 5; Art 4 of GDPR considers a wider range of data that are likely to be relevant to NHS records managers including "data concerning health", "biometric data" and "genetic data".
- There is a new right for data subjects to be informed how their data is being processed, which includes providing information about the legal

Information Commissioner's Office (Head Office)
Swyddfa'r Comisiynydd Gwybodaeth (Prif Swyddfa)
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510

basis for processing and informing data subjects how long their data will be retained by the organisation.

- The right of subject access is also changing. Under the current legislation a charge of up to £50 may be made to access health records, but GDPR is making access free in most circumstances. The shortened time for response will have a large impact across all parts of the NHS where records are held in many separate systems, media and physical locations, and should be checked by a relevant clinician prior to disclosure.
- There are new rights in relation to automated profiling which may impact upon screening or other health improvement type activities involving reviewing health records.
- Data Protection Impact Assessments will need to be undertaken in respect of much NHS processing, and Privacy by Design will need to be built in to all processing to show that you have considered and integrated data protection in to your activities.

B) Legal and Professional Obligations

The Legal and Professional Obligations section that starts on p7 could usefully cover other key issues such the Gender Recognition Act, witness protection schemes and adoption etc. Whilst these are currently covered in p33 of the document, they would benefit from greater prominence. Recent casework in ICO and discussions with the NHS Wales IG Managers Group has indicated that NHS Wales does not have clear nationally agreed policies or procedures on handling health records post gender change. Unless addressed at a level that encompasses all primary and secondary care records management systems, this lack of clear procedure will continue to be a high risk for future breach of both data protection and gender recognition laws.

The Commissioner would also like to see national emphasis on ensuring that all records containing personal data are within the view and control standards of each health board's central records management team. Casework again shows that in parts of NHS Wales there is risk posed by records containing personal data held in individual teams, such as frontline clinics or researchers. Such records are not appropriately linked into the Health Board's records management processes and therefore are at risk of not complying with the law, for example by missing demographic or clinical updates which could significantly impact on quality of care and on the rights of the individual as such data may not be

accessible to records management staff when responding to subject access requests.

C) Loss and Breach of Health Records

The GDPR will introduce significantly stronger requirements on organisations to report breaches of data protection, and therefore it would be helpful for the Records Management Code to cover this. In GDPR, a "breach" means a breach of security leading to the destruction, loss, unauthorised alteration, disclosure of, or access to, personal data. The Commissioner is very supportive of the National Intelligent Integrated Audit Solution which is being rolled out across NHS Wales' electronic systems to prevent and detect breaches relating to inappropriate access in secondary care. However, Wales still relies to a great extent on hard copy records, and very few parts of NHS Wales have any form of electronic / radio tagging system to track hard copy records. Therefore in many Health Boards a hard copy health record may go missing and this will not be identified until that record is next requested for clinical care purposes. The record is deemed "unavailable" and there is no way of knowing if it has been lost / stolen or whether it is safely – but inappropriately – locked in a medic's desk.

When a record is identified as "unavailable" the focus of the existing system is on recreating the record to ensure continuation of correct care – which is clearly hugely important. However, this approach entirely ignores the rights of the individual patient, and is also unlikely to comply with the GDPR requirements that relevant breaches must be reported to the Commissioner, investigated by the organisation in question and where appropriate the data subjects should be informed. Data subjects / patients have a right to know if their information has been breached in a way that could cause them harm, not least because they may need to take steps to protect their privacy and rights.

Any investigation by the Information Commissioner into such breaches would – amongst other things - consider whether the data controller knew, or should reasonably have known about the risk and if so, whether they had taken appropriate actions to mitigate that risk.

It should be noted that under GDPR, organisations will need to report relevant security breaches within 72 hours of identification. It is likely that the maximum financial penalties for such breaches in the public sector will rise from the existing £500,000 to €10,000,000 whilst failure to report a security breach will incur a further penalty. It should be further noted that breaches of other provisions of the GDPR can incur fines of up to €20,000,000.

Information Commissioner's Office
Swyddfa'r Comisiynydd Gwybodaeth

D) Devolution

The text of the IGA Code has been written for England and contains various references to legislation, organisations and guidance that may need to be reviewed for relevance in Wales.

Please contact Helen Thomas at the ICO's Cardiff Office on 01625 545298 if you would like to discuss any aspect of the above response.

7 February 2017