Welcome to the **twenty first** edition of the information governance bulletin

Our regular bulletin about information governance and the work of the IG transition programme

In this Edition...

Page 2: Revisions to EU data protection laws  
Page 7: The Caldicott Annual Report  
Page 4: HSCIC publishes code of practice

About this Bulletin...

*This bulletin sets out the work that NHS England is carrying out on behalf of the NHS to overcome the information governance (IG) issues created by the legal and organisational changes introduced by the Health and Social Care Act 2012.*

*This bulletin is written for anyone who uses data for secondary uses, such as commissioners inside NHS England and within CCGs, data analytics providers, those working in clinical audit, researchers, managers, clinicians, and patients.*
Welcome to the 21th edition of the IG Bulletin

Welcome to the first edition of the IG Bulletin of the New Year!

In this edition, we take a detailed look at what’s likely to be an important issue throughout 2015 – the proposed revisions to the European Union’s data protection laws, which could have a major impact on how the NHS collects and uses data.

We also have an update on how the NHS is responding to the Caldicott Annual Report, the new HSCIC Code of Practice – and an app to be avoided!

Stuart A Notholt
Editor

Revisions to EU data protection laws could have a profound impact on the NHS

Karen Thomson, Head of Strategic Information Governance for NHS England was a panellist at Forum Europe’s 5th Annual European Data Protection & Privacy Conference. The NHS European Office arranged for her to speak at this high-level data protection conference in Brussels on 9 December to share the potential impact of the revised legislation on the NHS with European officials and politicians. Here, Karen shares some thoughts on the issues.

The European Union has been working intensively on a new package of data protection legislation to ensure that EU citizens’ personal data is protected equally across all EU countries. The legislation, still under negotiation, will impact on the NHS, as it seeks to address the processing of personal data for health purposes including any new administrative requirements for data controllers and processors.

NHS England, along with the IG Alliance and coordinated by the NHS European Office, has been following the negotiations and speaking to leading EU officials and politicians to ensure that the NHS influences the revision of the new legislation. This is crucial for two key reasons: first, to ensure that patients’ data will be appropriately protected; and second, to be confident that our national ambitions for using data and technology to transform outcomes for patients and citizens – as outlined in the National Information Board’s (NIB) Personalised health and care 2020 strategy – will be achievable under the new legislative framework.

The critical concern for the NHS will be to maintain the flexibility to process personal data without the need to obtain explicit consent for every processing activity. This includes ensuring that those NHS organisations...
that de-identify data for use in secondary purposes (Health & Social Care Information Centre and accredited safe havens) will be able to maintain this function.

We are concerned that some of the current proposals may only allow regulated professionals to process sensitive personal data. If the NIB data and technology strategy is to be achieved, a number of NHS administrative and IT staff will need to have access to such information to de-identify data and perform data linkages. Although strict confidentiality clauses should be included in the employment contracts of these personnel, they will most likely not be from a regulated profession.

And an over-prescriptive definition of which professions will be allowed to process personal data for health purposes may hinder the development of better models of integrated care, which is very much at the heart of the NHS Five Year Forward View. Safe and effective care is dependent on relevant confidential information being shared among all members of the direct care team, not all of whom have regulatory bodies.

The controversial addition of the ‘right to be forgotten’ in the new laws could also affect health, and we are working to ensure the text is appropriately tailored for health purposes. Currently, unclear wording could allow patients a right to demand that parts of their medical records be deleted, which may not be in the patient’s best interest. The absence of a particular episode of care or test result could have a significant impact on clinical diagnosis and future care. And also represents challenges for clinical governance and medico-legal issues if the integrity of records is not maintained.

The new EU legislation could make it illegal for NHS organisations to charge a fee to cover costs when patients request copies of their paper medical records. Funds would be diverted from other services to cover these costs, which would be unhelpful in times of austerity.

The proposed new obligations of data controllers and processors takes a ‘one size fits all’ approach, which is difficult to apply across every sector, and across every EU member state. We are pushing to ensure the text maintains a level of flexibility. The legislation should not add costly administrative burdens on NHS organisations, particularly if these new requirements will not add an increased level of privacy for patients.

Finally, the new regulation could also have an impact on life-saving medical research.

While the original draft of the revision set out a broadly proportionate mechanism for protecting privacy, while enabling health and scientific research to continue, the European Parliament’s amendments significantly
reduce the scope of this research exemption.

The use of personal data in research without specific consent would be prohibited or become impossible in practice even under the Section 251 mechanism. Whilst consent is the appropriate lawful basis for most research, there are certain types of research that are just not feasible if consent is required. Examples could include:

- historical data where patients are untraceable
- research into child abuse where the parent (i.e., the person giving consent) could also be the abuser
- for research involving dangerous and severely personality disordered patients who may flip-flop on consent as a means of subverting the research
- research looking at the behaviour of clinicians and where seeking consent would change the behaviours being researched.

This would also put at risk significant European investments in genetics, cohort studies, biobanks, disease registries and the use of routinely collected data used to deliver real patient benefit.


WhatsApp ‘to be encrypted’

In our November issue, we warned of the dangers of using mobile apps that lack proper security features and that do not conform to NHS information governance standards.

A timely reminder has come with the news that the latest version of the very popular WhatsApp claims to have introduced ‘end to end encryption.’ (See http://www.bbc.co.uk/news/technology-30114346)

Whatever the other merits of WhatsApp, it should never be used for the sending of information in the professional healthcare environment. WhatsApp, which is owned by Facebook, is a consumer service, which does not have a service level agreement with users and has no relevant data security certification.

There is no valid reason for its use within the NHS. Only apps that have been specifically approved by NHS England should be used. We hope to have an update on this subject in a future edition.
NHS England and the Caldicott Annual Report

Dame Fiona Caldicott’s Annual Report to the Secretary of State on the implementation of the recommendations in her 2013 review highlights both the successes and challenges faced by the NHS since the re-organisation of the NHS in 2013. NHS England acknowledges its responsibility both to meet its own commitments but also to support the NHS in meeting the recommendations of the Review. NHS England also recognises that there is still much to do to achieve these aims. To that end, NHS England has initiated a Caldicott implementation programme to:

- deliver work on informing patients about how the NHS uses their personal and confidential information, and
- enable patients to access their GP records, make appointments and order repeat prescriptions online from March.

The laws and duties imposed on those who handle confidential health and care information are numerous and have become increasingly complex over recent years. Under the Health and Social Care Act 2012, the Health and Social Care Information Centre (HSCIC) is required to publish a Code of Practice, and organisations that handle confidential information about the provision of health and adult social care in England are required to have regard to it.

The Code applies to any organisation that collects, analyses, publishes or disseminates confidential information, ranging from GP practices and hospital trusts to commissioners and research organisations.

The HSCIC released a Guide to Confidentiality in Health and Social Care in September 2013. This provides patients and health and care staff with clear, accessible guidance on the handling of confidential information. This guide is available on the HSCIC website at www.hscic.gov.uk/confguide

The new Code of Practice aims to complete the picture by providing good practice guidance to those responsible (e.g., Board members) for setting and meeting organisational policy relating to the handling of confidential health information.
and care. The code is available online at www.hscic.gov.uk/cop

The Code will help organisations ensure that the right structures and procedures are in place to help front-line staff follow the confidentiality rules.

It is necessarily a legally precise document. However, the document clearly outlines the steps in the information-handling life cycle that organisations must, should and may take to ensure that confidential information is handled appropriately.