Welcome to the nineteenth 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: IG implications of the GMS contract
Page 3: Using apps to share data.
Page 4: Offshoring of data

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 19th edition of the IG Bulletin

In this edition we focus on some of the information governance issues in the new GMS contract. We also look at the risks posed by one example of new technology and some lessons learnt from recent issues.

I hope you find IG Bulletin useful. Do let me know if there is anything you would like to see featured in a future edition.

Stuart A Notholt
Editor

Information governance implications of the new GMS contract

The new contract between NHS Employers (on behalf of NHS England) and the BMA’s General Practitioners Committee (GPC) that will apply to GMS contractual arrangements in England from April 2015 includes a number of key changes having implications for information governance.

Most directly, the new contract calls upon the parties to actively promote the completion of the Health and Social Care Information Centre Information Governance Toolkit including adherence to the requirements outlined within it. This is asking General Practices to complete the IG Toolkit and meet the standard required: at least level 2 in each of the 13 (for 2014/15) requirements each year.

The challenge for many GPs is to complete the Toolkit, which is submitted in March each year, during one of their busiest periods. Feedback from GPs suggests that those that divide the work across the year (a little and often) makes the task less burdensome.

The IG Toolkit allows GP practices accurately to assess how they are managing patient data and the challenges they face in the use of protection of patient information. With an accurate assessment, GPs can target the work they need to do to meet their obligations.

As part of the drive to further empower patients and the public it has also been agreed to extend online access to medical records. From April 2015, practices will now be required to offer online access to all information that is held in a coded form within the patient’s medical record. The intention is to allow patient’s access to all of their record including those coded elements which will require further explanation for the patient to understand them.
Discussions are underway to ensure that GP software provision is configured to offer all coded data by default via the online service. GPs will have the option to withhold coded information where they judge it to be in the patient’s interests or where there is reference to a third party. Where free text is currently embedded within coded information, technical amendments to GP software will allow coded information to be separated from free text. GPs will be able to withhold such free text whilst still meeting the new contractual obligation to provide coded information.

This contractual amendment aligns record access by GPs with the expectations within legislation and government commitments to giving patients full access to their records. Whilst it does recognise the necessary safeguards for third parties and harm or distress to the patient, providing patients with coded information will require those codes and their context to be explained.

It has also been agreed that the GMS contract will be updated to set higher expectations for the number of appointments patients can book online, order repeat prescriptions electronically, and the number of electronic referrals made by for GP practices. The expectation on practices is that 60% of practices will be transmitting prescriptions electronically, and for 80% of elective referrals will be made electronically by the end of March 2015.

This is part of the push to ensure that wherever possible options are available that makes the best use of technology for patient choice and referrals from practices.

Achieving these objectives will require the strong leadership and enablement by NHS England, Clinical Commissioning Groups, provider organisations and the Health and Social Care Information Centre.

The NHS Employers’ contract website www.nhsemployers.org/gms provides details of the agreement (See www.nhsemployers.org/GMS201516.) Both this site and the NHS England’s dedicated GP contracts page (http://www.england.nhs.uk/ourwork/commissioning/gp-contract/) will be updated with details of implementation guidance, links to supporting legislation and standard contract documentation in time for these new arrangements to take effect from April 2015.

---

Risk alert – using apps to share data

With new technology, apps, and new ways of working emerging all of the time keeping pace with all of the possibilities is challenging. For organisations, clinicians and other staff is crucial to ensure that your use of
new technology meets the expected standard within the NHS and that any risks have been assessed as well as the potential benefits.

One recent BBC report featured a new app – ‘Figure 1’ – that has been developed to enable healthcare professionals to share clinical photographs of their patients for diagnostic or training purposes. (See http://www.bbc.co.uk/news/technology-29521986)

This report highlights a number of issues and problems with using technology of this nature. Some of these include:

- Currently, there is no assurance provided by the creators of this app regarding the physical storage, security and distribution of images submitted for use.
- Although patients’ faces are automatically obscured by the app, users must manually block identifying marks such as tattoos. In any case, anonymising images by blanking out the features does not represent an acceptable alternative to informed consent for the image’s use and may not prevent the individual being identified.
- The app claims that it does not access any patient records. This does not reflect what any image taken does. As clinicians will know, clinical photographs illustrate a patient’s medical condition or an aspect of their treatment, so they do form part of that patient’s confidential medical record. Such images, especially where anonymisation cannot be guaranteed, are subject to the same security and confidentiality considerations as any other medical record.
- The copyright of all clinical photographs produced by staff employed by one Trust is, in most circumstances, the property of that Trust and should not be transferred without permission to any other organisation.
- Information Security Management: NHS Code of Practice states that digital or printed X-rays, photographs, slides and imaging reports, outputs and images must be treated as an information asset (i.e., the same as paper or digital health records) and as such they are required to abide by all relevant laws and national guidance. This in particular means compliance with the Data Protection Act 1998 with regards to the taking, holding and using of patient images.

Here is a quick list of some basic questions:

- Does the technology use personal data (remembering
that this includes both audio and visual)?

- Do you have a lawful basis to use the information for that purpose?
- Does the patient understand what’s happening with their data (or image)?
- Where will the data be stored? Where are the data backups of that storage?
- Has my organization reviewed the app’s use and provided guidance or approval?

If you are not sure about the answers to any of these questions please speak to your organisation’s IG Team.

Medical staff wishing to share images with colleagues within the organisation for a second opinion or teaching must only do so through an approved system that meets the required standards covering such issues as security, audit and supports information governance best practices.

Staff access to their own or anyone else’s records - Just because you can does not mean you should!

A number of recent incidents have highlighted a worrying area of activity, where staff have been accessing their own, or a relative’s, records. Staff that need access to their own or anyone else’s records must go through the same process as anyone else. Whilst staff may have the capability to access records, and whilst a patient may be a relative and have given consent, it is important that they follow the procedure laid down by their organisation for access to patient data. Failure to do so exposes the staff member to the possibility of disciplinary action, or even action by the ICO for breach of the Data Protection Act.

For NHS Trusts should assess whether this is an risk in their own organisation and whether current staff training is adequate in managing this issue.

Offshoring of data

Various organisations have been asking for a steer from the Department of Health with regards to the additional offshoring of patient data.

Ministers have strongly indicated that they are not willing to relax the current prohibition on additional offshoring data associated with or linked to any centrally provided applications and services.

The option of introducing an exception process with each case being considered by Ministers, has also been ruled out.

Lessons learnt
Like most organisations, NHS England studies the Information Commissioner Office’s incident reports in order to consider the impact of particular incidents and the risk it faces in a similar incident occurring.

One incident in 2013 highlighted an issue of concern for all commissioners. The Information Commissioner’s Office was informed of a case where an NHS provider Trust shared seven discs holding patient data with a Clinical Commissioning Group (CCG). The discs contained descriptive patient data of over 40,000 patients (data subjects in terms of the Data Protection Act).

The discs were safely received, but the CCG found that the discs were not encrypted. Reassuringly, the discs were sent via recorded delivery to a named member of staff but without encryption this represented a security risk and a failure to meet NHS standards of information security.

There was also no record of the senior member of staff at the provider Trust, who sent the information having completed any information governance training. The ICO highlighted that monitoring of staff training, especially for senior staff, was lacking and was not part of a routine induction process.

The provider Trust has undertaken to ensure that all staff undertake mandatory data protection training upon commencement of their employment, and that completion of such training will be recorded and monitored to ensure compliance. This should already be part of their annual self-assessment within the IG Toolkit (requirements 201 and 112 for a starter). The Trust also agreed to set up a refresher programme to ensure that data protection training is updated at regular intervals.

The interesting bit for commissioners happened next. As part of his investigation, the Information Commissioner queried the legal basis on which the data was provided to the CCG. The commissioner could not provide a valid legal reason for the CCG to hold or access the patient data. The CCG had also asked for additional data fields, on top of the usual data set, without considering whether they were required creating a potential for providing excessive information.

The ICO noted that there was no information sharing agreement (nor any privacy impact assessment) that should have drawn out the issues around the lawfulness of the flow of data. Whilst not entirely relevant, as no lawful basis was found in this instance, this would have also drawn out the expectations around security. Accordingly, the Trust has undertaken to ensure that in future personal data are processed in accordance with the First (Fair and Lawful), Third (Relevant and not excessive) and Seventh (secure) Data Protection Principles in
Part I of Schedule 1 to the Data Protection Act 1988. The CCG was also lucky not to have failures against the Sixth (rights of the patient with regard to data) and Second (use for a specified purpose) highlighted to them. Critical amongst the Trust’s work will be a Privacy Impact Assessment in respect of any data sharing with the CCG or any other organisation. This will include consideration of the necessary legal basis for the provision of personal data and minimise the amount of data, in accordance with the purpose for its processing. The Trust will also shall ensure that appropriate information sharing agreements are in place and will maintain a register of agreements which it will keep under review.

The Information Commissioner’s Office is keen for all NHS organisations to consider any incidents, undertakings and enforcement action taken against NHS organisations. This forms part of the considerations when evaluating any further investigation against any NHS organisation. Trusts and Commissioners should take the opportunity to evaluate where they stand with the risks of secure data flows and the legal basis of each flow, do they have sufficient mitigation in place or is further action required.