IG helpdesk: embed.infogov@nhs.net

Issue 9

INFORMATION GOVERNANCE – DOPs COMMUNICATION

Topics covered:

- **Privacy Notices**
- **ICO Code of practice**
- **GDPR**
- **Illegally accessing patient records**
- **Advice on sending out correspondence**
- **Outcomes from visits to general practitioners and primary healthcare providers**
- **National Data Guardian Report**
- **Subject Access Requests**
- **Signature blocks**
- **IG Portal**
- **Training Modules**

Privacy Notices

Please find amended template but each individual practice must complete parts and add to it if patient information is used for any other reasons. Please note that privacy notices must be displayed on your website. Please find example privacy notice below.

GP Example Privacy Notice V2.docx

ICO Code of Practice

Please find link below to the ICO Code of Practice, the below document can also be found on the IG Portal.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

GDPR

Remember the GDPR comes into force on the 25th May 2018.

This checklist below highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently. It is important to use this checklist to work out the main differences between the current law and the GDPR.

https://portal.yhcs.org.uk/documents/67881/12147008/Preparing+for+the+GDPR+-+12+steps+to+take/d9a4f4c7-a64b-46ed-99d5-ec615989145f

Illegally accessing patient records

A former NHS administrator has been fined for unlawfully accessing patient records and was fined £200 for each offence, she was also ordered to pay £350 costs and a £40 victim surcharge.
Please find link to story below.

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/gp-surgery-administrator-fined-for-illegally-accessing-patient-records/

Advice on sending out correspondence to avoid incidents

A review of both internal and external incidents over the past year has highlighted that a common cause of breaches of the Data Protection Act and Confidentiality is still in the area of sending out correspondence whether this be by post, email, fax and when scanning documents to add them to records or to send to an authorised recipient. It was therefore felt it would be useful to reiterate the requirements when sending out documentation containing personal identifiable and sensitive information. Please find link below to the document which can be located on the IG Portal under the GDPR folder.

https://portal.yhcs.org.uk/web/information-governance-portal/information-governance-guidance-for-general-practice

Outcomes from visits to general practitioners and primary healthcare providers

In 2013/14 the ICO undertook 24 advisory visits at GP surgeries across England in order to get a better understanding of the processing they undertake and the circumstances that they operate in. This was in response to requests directly from surgeries and also working with a Clinical Commissioning Group (CCG) and a Practice Manager's forum. The ICO also conducted audits with out of hours primary care providers. Please find link below to the ICO document which can also be located on the IG Portal under general guidance and briefing folder.

https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/1934/advisory-outcome-report-gp-healthcare.pdf

No surprises" and reasonable expectations

The National Data Guardian (NDG) Dame Fiona Caldicott has often said it is important that there should be 'no surprises'. It's crucial to understand the boundary between what would and would not surprise people. This understanding should shape the way health and care professionals talk to people about how information is used. This is not just a matter of courtesy. It is also a question of law. It is important to remember that the boundary of what people reasonably expect is itself a restriction on the way information can lawfully be used. . Please find link below to the article.

https://www.gov.uk/government/speeches/reasonable-expectations

Subject Access Requests

Reminder to check the records before sending out

The Data Protection Act 1998 quite clearly states that before a copy of patient records is sent out it must be checked by a clinician for:

- Any references to 3rd parties
- Anything that could physically or mentally harm the patient or anyone else

These items must be redacted.

Remember currently fines for non-compliance are up to £500,000 and the Information Commissioner's Office has already fined a GP for non-compliance in this area.

Signature Blocks on emails

We in the eMBED Information Governance team love answering your queries but sometimes this is made difficult when emails are forwarded to us and the original sender's email address becomes 'lost' making it impossible to assist the original sender or obtain any additional information required.

We ask that you please amend your signature block to include your email and contact telephone number as well as ensure that your default signature is included in all replies and forwards by selecting 'auto sign' as Outlooks default is 'none'

Further instructions on how to amend your signature can be found here:

https://support.office.com/en-gb/article/Create-and-add-a-signature-to-messages-8ee5d4f4-68fd-464a-a1c1-0e1c80bb27f2

IG Portal

The IG portal is an invaluable tool for DOPs and contains template documents for toolkit compliance, an informative Blog, as well as a huge array of general IG information and links.

Come visit us at:

https://portal.yhcs.org.uk/web/information-governance-portal/home

The Data Security Awareness Level 1 e-learning training package, which replaces the Annual Information Governance (IG) training, is now live on https://nhsdigital.e-lfh.org.uk/ and via the Electronic Staff Record.

Data Security Standard 3 in the Caldicott 3 Review requires that all staff undertake appropriate annual data security training and pass a mandatory test. Therefore, if non-permanent staff have access to personal information they need to complete the annual training.

Training modules

The training is split into four learning modules with an additional "Welcome module". Each module takes 12-14 minutes to complete and concludes with an assessment.

The modules can be taken in any order and the system will record the pass marks and issue a certificate on successful completion of the five modules.

The Caldicott requirements are that 95% of all health and care staff achieve an 80% pass mark.

The topics covered in the four modules are:

1. Introduction to security awareness
2. Information and the law
3. Data security - protecting information
4. Breaches and incidents

Level 2 and Level 3 learning material will be released over the coming months.

Please find links below to the support website for registration, access to the training and ongoing support
http://support.e-lfh.org.uk/e-lfh-support-home

Specifically for logging in, this link is useful:-
http://support.e-lfh.org.uk/get-started/logging-in-out/

The eMBED IG Team are here to help and support you in all matters relating to confidentiality, information governance and information security.

Contact us any time at: **eMBED.infogov@nhs.net**