IG helpdesk: embed.infogov@nhs.net

Issue 13/14

INFORMATION GOVERNANCE – DOPs COMMUNICATION

Topics covered:

- **GDPR**
- **IG Toolkit**
- **Enforcement taken by the Information Commissioner's Office (ICO)**
- **Phishing**
- **Training Modules**
- **IG Portal**

Please note that you need to CTRL+CLICK to access the links

General Data Protection Regulation (GDPR)

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 and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR.

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

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Or visit the IG Portal's GDPR folder for more help and assistance.

IG Portal GDPR Folder

Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules: In most cases you will not be able to charge for complying with a request. You will have a month to comply, rather than the current 40 days. You can refuse or charge for requests that are manifestly unfounded or excessive. If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month. If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas. The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation. When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language. The ICO's Privacy notices code of practice reflects the new requirements of the GDPR. Please see link below to the ICO Privacy Notices Code of Practice.

ICO Privacy Notices Code of Practice

IG Toolkit v14.1

The deadline submission date for this is 31st March, however we always recommend trying to submit earlier to avoid the last minute rush and the technology glitches this sometimes causes.

If you need documents then visit our portal https://portal.yhcs.org.uk/web/information-governance-portal/home or if you have any questions or queries then contact our helpdesk EMBED.Infogov@nhs.net

Please be aware that after this submission the toolkit will completely change for 2018/19 and is the Data Security and Protection toolkit. We will be sending out advice and guidance on this and update documents on the portal for you to use.

Enforcement taken by the Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) has the right to fine up to £500,000 for breaches of the data protection act. Under the new General Data Protection Regulation (coming into force on May 25th 2018) this will rise to fines of up to €20,000,000.

It is important to remember that the ICO does not generally fine for the breach itself but for not having robust systems and processes in place to prevent breaches happening. It is vital that staff are trained in all aspects of confidentiality and information security and that the correct policies are in place.

- A former local authority education worker who illegally shared personal information about schoolchildren and their parents has been prosecuted.
  Samira Bouzkraoui, 24, took a screenshot of a council spreadsheet concerning children and their eligibility for free school meals before sending it to the estranged parent of one of the pupils via Snapchat, whilst working for Southwark Council.
  The image included the names, addresses, dates of birth and National Insurance numbers of 37 pupils and their parents. She also sent a copy of a school admission record relating to another child. She was fined £850 and was also ordered to pay £713 costs.

- A former worker at an accident repair firm who downloaded and sold the personal data of motorists to nuisance callers has been fined.

  Phillip Bagnall, 33, of Scotta Road, Eccles, Greater Manchester, was an employee of Nationwide Accident Repair Services Limited (NARS) when he was found to be accessing suspicious volumes of customer data from a laptop at home outside of work hours.

  During a week that Bagnall's accesses were monitored, he accessed the data of 2,724 customers without his employer's consent. Customers whose data was accessed subsequently received unsolicited and at times aggressive marketing calls regarding their accidents and they were asked whether they wanted to pursue legal claims.

  The defendant pleaded guilty to unlawfully obtaining data in breach of s55 of the Data Protection Act 1998 when he appeared at Manchester and Salford Magistrates' Court. A further charge of unlawfully disclosing data was also admitted and taken into consideration. Bagnall was fined £500 and was also ordered to pay £364 costs and a £50 victim surcharge.

- A Kent man who posted sensitive police information on Twitter has appeared in court after he admitted breaking the Data Protection Act.

  William Godfrey, 30, of Bull Lane, Bethersden, had previously been in a relationship with a probationary officer, and came into possession of a USB stick containing the data. In July 2016, he tweeted the name and address of a vulnerable adult, along with details of their health and sexual life, to the accounts of the Information Commissioner's Office (ICO), the Independent Police Complaints Commission and Surrey Police.

  That same day, he emailed the ICO threatening to publish a 40-page document containing personal data, which included the details of a victim of a sexual offence, and became involved in a Twitter exchange with an independent user who saw his tweet and warned him that he was breaking the law.

  The ICO contacted him to ask him not to publish the material. Godfrey later failed to attend a meeting to hand over the USB stick and Surrey Police eventually had to take out an injunction to retrieve it.

  Godfrey admitted two offences of unlawfully disclosing personal data in breach of s55 of the Data Protection Act when he appeared at Maidstone Crown Court, on Wednesday 17 January 2018.

  He was sentenced to a 12-month conditional discharge, in part because he had been placed on stringent bail conditions, including an electronic tag, before the hearing. He was also ordered to pay £150 costs and a £15 victim surcharge.

Phishing

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

Common Features of Phishing Emails

Too Good To Be True - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people’s attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems too good to be true, it probably is!

Sense of Urgency - A favourite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organisations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.

Hyperlinks - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.

Attachments - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.

Unusual Sender - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

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

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/

Please note any queries should be directed to e-LFH at the link above.
The IG team do not facilitate this e-learning.

IG Portal

The IG portal is an invaluable tool for Dentists, Optometrists & Pharmacies and contains template documents for toolkit compliance, an informative Blog and lots of information about GDPR, 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