IG helpdesk: embed.infogov@nhs.net

Issue 7

Have you submitted your Information Governance Toolkit yet? Deadline is 31st March.

INFORMATION GOVERNANCE – GP and DOP COMMUNICATION

Topics covered: Confidentiality: good practice in handling patient information, Confidential Waste, Targeted Phishing Attack, CareCERT Alerts Summary.

Confidentiality: good practice in handling patient information

The General Medical Council has updated **Confidentiality: good practice in handling patient information** This guidance clarifies the public protection responsibilities of doctors; the importance of sharing information for direct care; the circumstances in which doctors can rely on implied consent to share patient information for direct care; and the role that those close to a patient can play in providing support and care.

http://www.gmc-uk.org/Confidentiality2017.pdf_69037815.pdf

Confidential Waste

All staff have a duty of confidentiality to safeguard personal and confidential information during the course of their work. This is not just a contractual obligation but is a requirement of the Data Protection Act 1998.Confidential waste is defined as '*waste containing personally-identifiable Information' or 'waste which is business sensitive'.*
It is the responsibility of all staff to ensure information they are handling is destroyed effectively and securely.
All confidential paper records/documents that have reached the end of their life cycle should be destroyed using one of the following methods:

- Paper records should be destroyed using a shredding device designed to cross cut material to ensure shredding cannot be reconstructed. Staff are responsible for ensuring records are destroyed adequately and in such a way that protects the security of the information contained within them.

- Locked confidential waste bins should be located throughout the premises and it is the responsibility of every member of staff to ensure that confidential waste is disposed of in the correct receptacles, the confidential waste container is locked at all times and the key to the confidential waste bin is kept secure. Items should not be stored elsewhere awaiting disposal but should be dealt with immediately.

Advice should be sought from your IT service provider regarding the destruction of IT equipment and electronic media. You should ensure that you receive certificates/proof of any destruction.

Targeted Phishing Attack

NHS Digital have been made aware of some targeted (spear) phishing emails being sent to CCGs and GPs. Attackers are setting up email accounts on webmail services, such as Hotmail, in the name of an employee at a CCG/GP practice or supplier.

The attacker uses the email account to target a staff member at the CCG/GP (for example a GP Practice Manager) to convince them to transfer funds to a UK bank account.

Generally, untargeted spam emails containing malicious attachments are easy for the trained eye to spot, whereas targeted (spear phishing) campaigns can be much more convincing. The attacker establishes a dialogue and the user expects a response containing instructions, a link or an attachment which they are likely to act upon.

Remediation: If you receive an email from a familiar organisation or contact which you believe to be suspicious, such as an unusual payment request:

- Do not open attachments or follow links
- Validate the request by contacting the organisation or person through normal established channels (e.g. make a phone call or manually navigate to the organisation's website)
- Report all suspected spam to NHSmail via spamreports@nhs.net for analysis and blocking. See the Cyber Security Guide for details on reporting.

CareCERT Alerts Summary

The CareCERT Alerts summary summarises the threats which have been received over the past few months. Please click on the link below to view the summary.

CareCert Cyber Alerts Summary - Jan 2017