IG helpdesk: embed.infogov@nhs.net

INFORMATION GOVERNANCE – GP COMMUNICATION

Topics covered: Caldicott Guardian Manual, The Little Book of Cyber Scams, IG Toolkit, IG Portal, Data Protection Principle 7

New Caldicott Guardian Manual

The UK Caldicott Guardian Council has published an updated manual for Caldicott Guardians, this manual of good practice is intended to help Caldicott Guardians address their duties.

It includes information regarding Caldicott principles, legal &ethical aspects of the role, Data Protection Act principles, information sharing & disclosure and the use of patient information in research.

It also includes a checklist for new guardians, sources of help & guidance and details of key legislation.

A manual for Caldicott Guardians

Little Book of Cyber Scams

This is the first edition of the Little Book of Cyber Scams; this booklet has been developed to assist you to take the necessary steps to defend your business and your customers against cyber criminals.

..\December comms\little-book-cyber-scams.pdf

IG Toolkit v14

The deadline for submission for the IG Toolkit is 31st March so we would recommend you aim to complete by the end of February.
You should ensure that you have all the correct documentation and evidence in place so that you are able to submit in a timely manner as submission is mandatory.

IG Portal

The IG Portal link below lists all the required documentation for a General Practice to complete the Information Governance Toolkit.

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

Data Protection Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised.

In particular, you will need to design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach.
You must be clear about who in your organisation is responsible for ensuring information security. You must make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff and be ready to respond to any breach of security swiftly and effectively.

Access to patient systems

Remember that you are the Data Controller for all the patient information that you hold. This means that you are legally responsible for protecting it.

Be very cautious when granting access to these systems for any purpose other than direct care.

If in doubt contact the IG helpdesk

EMBED.Infogov@nhs.net