IG helpdesk:
mailto:embed.infogov@nhs.net

Issue 18

INFORMATION GOVERNANCE – DENTIST, OPTOMOTRISTS & PHARMACY COMMUNICATIONS

Topics covered:

- **Data Security and Protection Toolkit**
- **E-learning**
- **Instant Messaging**
- **Incident Reporting**
- **Enforcement taken by the ICO**

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

Data Security and Protection Toolkit

All organisations should now be registered for the new toolkit and ideally be well on the way to completion and submission. Final submission date is 31.3.19 but early submission is recommended. IT evidence required is now available on the Embed IG portal:

DSPT IT evidence

Reports are being produced monthly on the status of each practice and will be made available to CCGs and NHS England. Please ensure that you have checked that you are only completing the mandatory sections within the toolkit, an action plan which only shows the mandatory items is available on the portal:

Mandatory Evidence

e-learning

The new data security elearning is now on the e-lfh web site:

https://portal.e-lfh.org.uk/login

Health Education England e-Learning for Healthcare (HEE e-LfH) has re-designed the Statutory and Mandatory Training e-learning sessions and eAssessments to be combined into a single package. This update will enable users to easily access both the knowledge content and e-Assessment in one session.

As part of this update to the Statutory and Mandatory Training programme, they have also updated the Data Security Awareness Level 1 session and eAssessment to include General Data Protection Regulations (GDPR) and social care updates.

If you are part way through completing these programmes, please be aware that the previous courses will remain accessible within an archive folder until 31 March 2019; enabling users and local administrators to access historic certificates and report on learning history.

Instant Messaging

New guidance for the NHS will help doctors, nurses and other staff use instant messaging safely to co-ordinate patients' care during emergencies. Medics have turned to communication channels such as Whatsapp to deal with emergency situations like the Croydon tram crash, Grenfell Tower fire and terrorist attacks in London Bridge and Manchester Arena.

Simple steps that staff should take include:

- Only using apps and other messaging tools that meet the NHS encryption standard
- Not allowing anyone else to use their device
- Disabling message notifications on their device's lock-screen to protect patient confidentiality
- Keeping separate clinical records and delete the original messaging notes once any advice has been transcribed and attributed in the medical record.

https://www.england.nhs.uk/2018/11/instant-messaging-services-a-vital-part-of-the-nhs-toolkit-during-a-crisis/

Incident Reporting

The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. An organisation must notify a breach of personal data within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay.

Those breaches that also fulfil the criteria of a NIS notifiable incident will be forwarded to the DHSC where the Secretary of State is the competent authority for the implementation of the NIS directive in the health and social care sector. The Information Commissioner remains the national regulatory authority for the NIS directive.

For urgent security related incidents that require immediate assistance and support an organisation is advised to contact the Data Security Centre (formerly known as CareCERT) helpdesk immediately on 0300 303 5222 or contact enquiries@nhsdigital.nhs.uk . As previously stated, this tool is for notification and local incident management must still be carried out.

The 72 hours starts when an organisation becomes aware of the breach which may not necessarily be when it occurred. An organisation must have a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised. This means that once a member of staff or the public has reported a breach this is the point that an organisation is aware. The actual incident may have occurred some hours, days or weeks previously, but it is only when an organisation is aware that the breach has occurred that the 72 hours to notification period starts.

Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

In the event that the Data Security and Protection Incident Reporting Tool is unavailable, users may choose to either report the incident via the ICO helpline on: 0303 123 1113

(ICO normal opening hours are Monday to Friday between 9am and 4.30pm) or report when the Data Security and Protection Incident Reporting tool is available noting the reasons for delay in the relevant part of the form.

Action taken by the ICO

ICO fines Uber £385,000 over data protection failings

The Information Commissioner's Office (ICO) has fined ride sharing company Uber £385,000 for failing to protect customers' personal information during a cyber-attack.

A series of avoidable data security flaws allowed the personal details of around 2.7million UK customers to be accessed and downloaded by attackers from a cloud-based storage system operated by Uber's US parent company. This included full names, email addresses and phone numbers.

The records of almost 82,000 drivers based in the UK – which included details of journeys made and how much they were paid – were also taken during the incident in October and November 2016. The ICO investigation found 'credential stuffing', a process by which compromised username and password pairs are injected into websites until they are matched to an existing account, was used to gain access to Uber's data storage.

However, the customers and drivers affected were not told about the incident for more than a year. Instead, Uber paid the attackers responsible $100,000 to destroy the data they had downloaded.

London company fined after 14.8m spam texts sent

London-based firm Tax Returned Limited has been fined £200,000 by the Information Commissioner's Office (ICO) for sending out millions of unsolicited marketing text messages.

The ICO's investigation found that, between July 2016 and October 2017, the company broke the law by sending 14.8 million marketing text messages without valid consent through a third party service provider.

As the instigator of the campaign, Tax Returned should have taken reasonable steps to make sure the data they obtained complied with the Privacy and Electronic Communications Regulation (PECR), which includes getting specific, prior consent from people receiving the messages. The firm also claimed that some of the consents were received through generic third party consent found on privacy policies of certain websites.

However, the ICO found that the wording of the policies was not clear enough and that neither Tax Returned nor the third party service provider were listed on most of those privacy policies.

The ICO has also served an enforcement notice on Tax Returned, ordering the firm to stop its illegal marketing activity.

Come visit us at:

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

or contact the IG Helpdesk

embed.infogov@nhs.net