this

IG Newsletter

Issue 12 | May 2023

NHS
The Health Informatics Service

GP Communications

Contents

compassionate care

Regulatory Guidance

Data Security and Protection Toolkit

The Data Security and Protection Toolkit is an online self-assessment tool that allows health and social care organisations to provide assurance that they are undertaking good data security and that personal information is handled correctly.

The deadline for the Data Security and Protection Toolkit is 30th June 2023, evidence will be circulated shortly to support you with completion.

Incident Reporting
The Data Security and Protection Toolkit includes a tool for reporting data security incidents to the Information Commissioner's Office, the Department of Health and Social Care and NHS England.

Organisations 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.

Once you have logged onto the DSPT, you will be asked a series of questions relating to the incident, you will have the chance to review your answers before you submit the incident. You don't have to complete the report in one go but you do have to complete the report within 72 hours. Depending on your responses, the information may be escalated to the Information Commissioner's Office.

Example of some DSPT reported breaches

1. A member of staff accessed her family's medical records and then divulged confidential information therefore the member of staff abused their level of access and obtained information without a legitimate reason.
2. A member of staff uploaded several photos of patients receiving medical treatment plus some pictures of medication showing patient identifiable information to their personal Instagram account.
3. A member of staff had their car stolen whilst working which contained some patient blood samples and paperwork containing patient identifiable information.

Near Misses
A near miss is where a breach could have occurred if an incident had developed or been left. Reporting near misses helps your organisation consider changes to ensure that information is kept secure

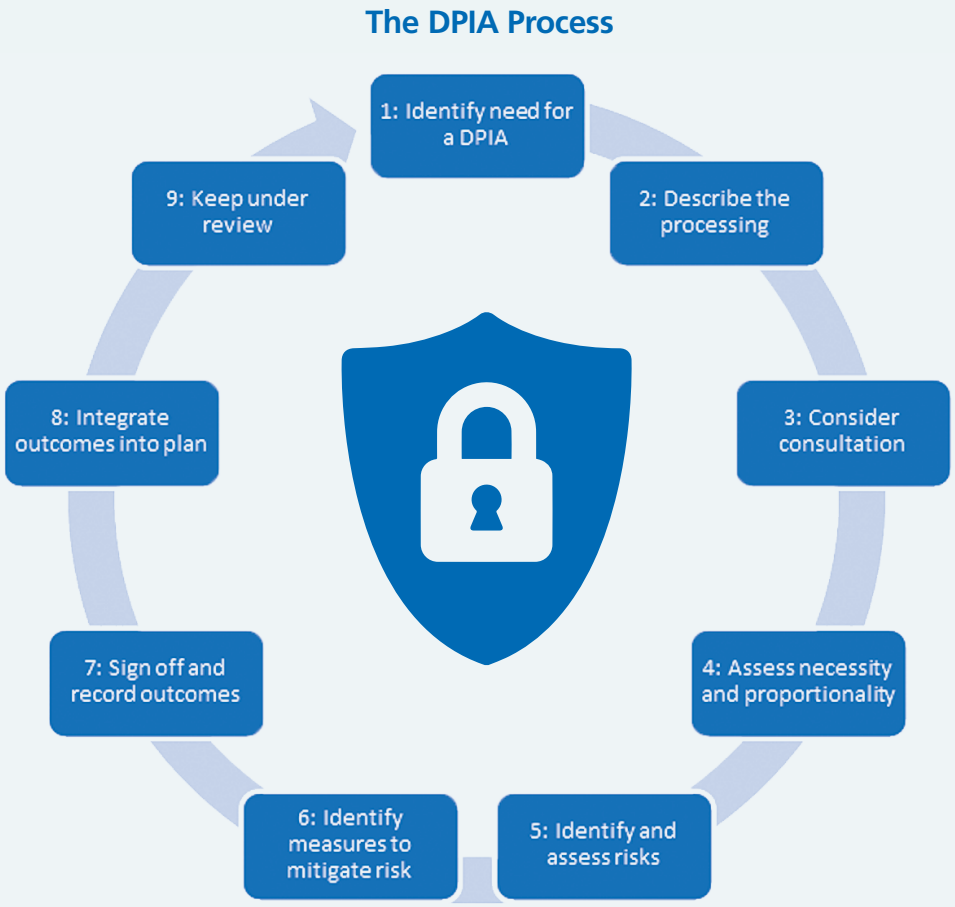
Example of near misses
Leaving patient records unsecured in a main hospital corridor used by the public

A patient is nearly given someone else's medication; however, the nurse realises the mistake and does not give the patient the medication.

A Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA before beginning any type of processing that is "likely to result in a high risk". This means that although you have not yet assessed the actual level of risk, you need to screen for factors that point to the potential for a widespread or serious impact on individuals. A DPIA does not have to indicate that all risks have been eradicated but it should help you document them and assess whether remaining risks are justified. A DPIA allows you to analyse your processing and helps you to identify & minimise data protection risks.

An effective DPIA can bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals. It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise. You should see it as an ongoing process that is subject to regular review.



Information Governance Issues

Latest Action Taken By The ICO

ICO reprimands Surrey Police and Sussex Police for recording more than 200,000 phone calls without people's knowledge

The Information Commissioner's Office (ICO) has issued a reprimand to both Surrey Police and Sussex Police, following the rollout of an app that recorded phone conversations and unlawfully captured personal data.

In June 2020, the ICO became aware that staff members across both police forces had access to an app that recorded all incoming and outgoing phone calls. 1,015 staff members downloaded the app onto their work mobile phones and more than 200,000 recordings of phone conversations, likely with victims, witnesses, and perpetrators of suspected crimes, were automatically saved.

The ICO considered it highly likely that the app captured a large variety of personal data during these calls and it considered that the processing of some of this data was unfair and unlawful. Police officers that downloaded the app were unaware that all calls would be recorded, and people were not informed that their conversations with officers were being recorded.

Asif Iqbal Khan

A former employee of the RAC has been prosecuted for obtaining the personal data of individuals involves in road traffic collisions after 21 drivers were harassed by claims companies.

Asif Iqbal Khan, 42, was fined £5,000, ordered to pay court costs of £937.40 and a victim surcharge of £170, after pleading guilty to two counts of data theft following an investigation from the Information Commissioner's Office.

The investigation revealed he had stored data from 272 separate traffic incidents on phones he owned, an order was made under s153 Sentencing Act 2020 for deprivation of the two phones. Mr Khan was working as a customer solutions specialist when in 2019 the RAC received complaints from suspicious drivers who had received calls from claims companies in January of that year.

A review by the RAC looked at how the information was obtained and found that Mr Khan was the only person who had access to the details of all 21 crash victims.

Appearing at Dudley Magistrates' Court, Mr Khan pleaded guilty to two counts of data theft in breach of section 170 of the Data Protection Act.

Martin Swan

A former 111 call centre advisor has been found guilty and fined for illegally accessing the medical records of a child and his family.

Martin Swan, 56, from Pinner, London, worked as a service advisor at the NHS 111 call centre in Southall when he illegally accessed the records.

A complaint had been raised against Mr Swan, following a disagreement during a 111 call over the distance to a medical centre, prompting him to access the records of the complainant, the complainant's child and two other relatives.

Mr Swan accessed the personal records without consent or a legal reason to do so and produced screenshots of the child's patient notes at an internal investigation meeting in June 2016. He proceeded to contact the father with accusations of falsifying events and was dismissed for gross misconduct in November 2016. He contacted the father once again in January 2017, threatening to report him for neglect.

Following the investigation from the Information Commissioner's Office, Mr Swan pleaded guilty to five counts of unlawfully obtaining personal data in breach of Section 55 of the Data Protection Act when he appeared at Uxbridge Magistrates' Court on 15 February 2023. He was fined £630 with a victim surcharge and court costs totalling £1,093.

Round up of General IG News Items

Template Policies and Resources for DSPT

Digital Social Care have developed a range of template policies and resources to help you to improve how you keep information safe. These resources are regularly quality assured and reflect the most recent requirements.

These resources can help you to meet your obligations on data security and protection and to complete the Data Security and Protection Toolkit (DSPT).

Please find attached link to these templates - **Template Policies and Resources for DSPT - Digital Social Care**

this

NHS
The Health Informatics Service

Making contact with the IG and RA Teams

You can log a query/issue with the IG and RA services by logging a job via the The Health Informatics Service Help Desk

Bradford GP Service Desk 0345 268 2600
(between 7:30am and 18:00pm Monday to Friday)

All other areas GP Service Desk 0845 127 2600
(between 7:30am and 18:00pm Monday to Friday)

You can contact the IG team via their shared mailbox at:
this.informationgovernance@this.nhs.uk

Or log a call directly through Remedy on Demand:
rod.this.nhs.uk

Let's make THIS work for you!

01484 355420

contact-us@this.nhs.uk

@thisnhs

the-health-informatics-service

thisnhs

www.this.nhs.uk

NET Promoter Score

How likely are you to recommend us to a colleague or friend?

Detractors							Passives		Promoters	
0	1	2	3	4	5	6	7	8	9	10
Not at all likely							Neutral			Extremely Likely

NPS = **% of PROMOTERS (9's and 10's)** - **% of DETRACTORS (0 to 6)**

"Companies with the most efficient growth engines operate at an NPS efficiency rating of 50 to 80%. The average firm sputters along at an NPS efficiency of only 5 to 10%." *

Our latest NPS score is: **April 2023** **+82.7%**

* www.netpromotersystem.com