DISCOVER 3 series

Brought to you by salts academy international

Discover Series Suggested Reading List

session 1:

Data Protection – do you know enough?

Data Protection Training Salts Healthcare Limited Nurses and Data Protection Law

Data Protection Law in the UK

The key piece of legislation in is the General Data Protection Regulation, known as the GDPR. The Data Protection Act 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. The Data Protection Act sits alongside the GDPR and tailors how GDPR applies in the UK.

Data Protection law in the UK is regulated by the Information Commissioner's Office (known as the 'ICO'). The ICO are responsible for overseeing data protection law in the UK, investigating any issues, and enforcing compliance by issuing fines and enforcement notices where necessary.

The ICO continue to develop and produce guidance notes to assist individuals in navigating their way through data protection law. The guidance notes on the ICO's website convey a practical approach and answer FAQs. The ICO's website also have sections specifically targeted at health data which may be particularly helpful to you.

Penalties and Enforcement

Under the GDPR, the ICO's authority to issue fines have been substantially extended. The ICO can now issue fines of £17.5m OR 4% of annual worldwide turnover – whichever is higher! Previously the ICO could only issue fines of up to £500,000. This illustrates the importance of taking data protection compliance seriously as the consequences could be severe.

In most cases, the ICO will fine the organisation for non-compliance. However, it is possible in certain circumstances for the specific individual responsible to be fined or prosecuted.

Examples of recent ICO enforcement:

- Ticketmaster were fined £1.25 million for failing to protect customers' payment details;
- Marriott International were fined £18.4million for failing to keep millions of customers' personal data secure. It was estimated that 339 million guest records worldwide were affected following a cyber-attack in 2014;
- Doorstep Dispensaree, a London-based pharmacy, were fined £275,000 for failing to ensure the security of sensitive types of personal data, including health information. Approximately 500,000 documents were left in unlocked containers at the back of its premises in Edgware. The documents included names, addresses, dates of birth, NHS numbers, medical information and prescriptions belonging to an unknown number of people;
- Kim Doyle & William Shaw – Kim Doyle, a motor industry employee was prosecuted for passing the personal information of service users to a William Shaw, a Director of an accident claims management firm without authorisation. Kim Doyle was sentenced to eight months' imprisonment, suspended for two years. William Shaw was also sentenced to eight months' imprisonment, suspended for two years and both were also each ordered to carry out 100 hours' unpaid work and contribute £1,000 costs. Kim Doyle must also pay a benefit figure of £25,000 and Shaw must pay a benefit figure of £15,000. Both will face three months' imprisonment if the benefit figures are not paid within three months.

The above examples confirm that the ICO can take enforcement action against organisations of all sizes and individuals in their personal capacity. Some of these cases have been handled under the old data protection law (due to when the issue actually occurred), had they been dealt with under the new law, the fines might have been even greater.

Individuals whose personal data has been treated unlawfully can also make a direct claim for compensation through the courts.

In addition to the potential financial consequences, there is also a risk of reputational damage where things go wrong. The ICO publish details of enforcement action they have taken on their website, and claims for compensation in the courts may be reported in the press.

What is “personal data”?

The whole purpose of the GDPR and Data Protection Act is to protect personal data.

Personal data is any information relating to an identified or identifiable person. If the information identifies a person, either directly or indirectly, it will be ‘personal data’. Examples include:

• Name; Date of Birth; Contact information – addresses (postal and email); telephone numbers

• Photographs, medical records

• CCTV images; telephone recordings; online identifiers.

This is not an exhaustive list but gives an idea of the types of information that comprises personal data.

An opinion about someone can constitute personal data. This could include an opinion on someone’s medical condition or lifestyle. In short, almost anything and everything about a living person has the potential to be caught by the GDPR.

‘Special category data’ is sensitive personal data, which benefits from additional protection under the legislation. This includes health information. For the healthcare industry, it is even more important that this type of information is kept safe and secure and handled in accordance with data protection legislation.

Examples include:

- racial or ethnic origin;
- political opinions, religious or philosophical beliefs;
- trade union membership;
- genetic data, biometric data and health data;
- sex life or sexual orientation data.

GDPR Principles

Article 5 of the GDPR sets out seven key principles:

• Lawfulness, fairness and transparency

• Purpose limitation

• Data minimisation

• Accuracy

• Storage limitation

• Integrity and confidentiality (security)

• Accountability

salts academy international

These are the key points that must be taken into account whenever you collect or process personal data, whether this relates to patients, their families, or anyone else whose personal data that might handled as part of your role.

Lawfulness, fairness and transparency:

When collecting or using personal data, there must be valid grounds for doing so as provided for under the GDPR, known as the 'lawful basis for processing'.
For the most part, this will be dealt with within privacy policies and notices made available to patients in connection with the care they are receiving.
A privacy policy should set out details of what types of personal data are collected, how the information is used, and the 'lawful basis' for the collection and processing of the information. There are six lawful
This guidance note has been prepared based on the law as of 19 October 2021. It is provided for information purposes only. It is not a substitute for legal advice in relation to a specific situation.
bases available under the GDPR. As a nurse, you should familiarise yourself with the applicable privacy policies and notices issued to your patients and ensure that you are handling personal data in accordance with this documentation.
Personal data must only be used in a way that is fair and that is not unduly detrimental, unexpected or misleading to the individuals concerned.
You must be clear, open and honest with people about how their personal data will be used. As above, the necessary privacy information should generally be communicated to individuals by way of privacy policies and notices.
It is therefore fundamental that personal data is only processed as set out in the relevant privacy policies and notices and any new types of processing of personal data must be authorised by the Data Protection Officer or other appropriate individual.

Purpose limitation:

When collecting personal data from an individual, there must be a purpose for requiring that information.
Subject to exceptions, the purpose limitation principle prevents you from then using that personal data for another purpose – you need to be clear with people from the start what you will use their personal data for, and only use it in that way.

Data minimisation:

Under this principle, you must ensure that the personal data you are processing is:
1. adequate – sufficient to properly fulfil your stated purpose;
2. relevant – has a rational link to that purpose; and
3. limited to what is necessary – you do not hold more than you need for that purpose.

Do not ask people for personal data that you do not need. For example, if you are required to take a photograph of a patient, ensure that you only capture the relevant area and keep family members or visitors out of the shot. Remember – the more data you hold, the more data you have to protect!

Accuracy:

Reasonable steps should be taken to ensure the personal data held is not incorrect or misleading and if it is discovered that personal data is incorrect or misleading, reasonable steps should be taken to correct or erase it as soon as possible. If a patient or family member informs you know that their personal details have changed, you should take steps to update this on your systems without delay, or you could be breaching the accuracy principle.

Storage limitation:

Personal data must not be kept for longer than it is needed and you need to be able to justify why you are holding personal data. This will depend on your purposes for holding the data and there may also be applicable regulations or policies requiring you to retain certain types of information for a specific length of time.

Integrity and confidentiality (security):

Appropriate security measures should be in place to protect the personal data you hold. This is also known as the 'security' principle.

The ICO have been keen in taking enforcement action under this principle and some of the examples considered above related to situations where the ICO have taken action where organisations have failed to adequately protect personal data.

Applying this principle to your day to day...

If a patient sends you a message or picture electronically, you should take steps to ensure that this is received and stored securely. Encourage patients to contact you via your work devices, which you and your employer can ensure are password protected and appropriately secured.

This guidance note has been prepared based on the law as of 19 October 2021. It is provided for information purposes only. It is not a substitute for
legal advice in relation to a specific situation.

Remember that use of third party platforms or social media may not always be secure or reliable. If a patient does send you a message or image by way of a third party platform, you may need to store this in an alternative format, to ensure that it is stored securely and reliably. Speak to your employer if you are unsure of the authorised platforms in which you can safely receive and store information. Avoid the use of personal devices unless the use of these for work purposes has been authorised by your employer and remember that even if you do not have a patient's number saved in your phone, they may still be identifiable by way of their telephone number or other electronic identifier.

DO's and DON'T's when using an electronic device for processing:

DO: ensure that you use work issued devices with appropriate security measures.

DON'T: use personal devices for work purposes unless this has been authorised expressly and you are confident that they are appropriately secured.

DO: only take video or telephone calls from patients in a private space where you can maintain confidentiality.

DON'T: take calls from patients in public places where sensitive information may be overheard.

Accountability:

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

You must have appropriate measures and records in place to be able to demonstrate your compliance.

Some of these principles will largely be more applicable to your employer but as a nurse, you should bear in mind and act in accordance with the principles considered above whenever you are dealing with personal data.

Rights of Data Subjects:

Whilst the principles are imperative to the current data protection regime, the GDPR extends further than this and gives individuals certain rights in respect of their data. These are as follows:

- The right to be informed – individuals have the right to know how their personal data is processed, and is predominantly dealt with by way of the privacy policy.
- The right of access – individuals have the right of access to their own personal data (subject to certain exemptions).
- The right to rectification – if the information held about someone is wrong, they have the right to ask you to correct it.
- The right to erasure – in some circumstances, individuals have the right to ask you to erase the personal data you hold about them.
- The right to restrict processing – in certain circumstances, individuals can ask you not to use the personal data you hold about them.
- The right to data portability – individuals can obtain their data in a portable format that they can use for other purposes.
- The right to object – individuals can object to some types of processing, for example they can object to their data being used for marketing purposes.
- Rights in relation to automated decision making and profiling – this applies where you are using someone's personal data to profile them or make automated decisions.

If you receive a request from a patient or any other individual to exercise any of the rights listed above, you must escalate this request to the appropriate member of staff within your team as soon as possible as there are statutory time limits for responding to such requests. You should not respond to any data protection related requests directly unless you have received appropriate training and this forms part of your role.

The most commonly exercised right is 'the right of access'. It is important to note that an individual does not have to use the word 'access' or refer to data protection legislation in order for a request to be valid – any request for personal information may constitute a subject access request for the purposes of the legislation. A request can be made in any format including; in writing, verbally or even by social media. It is also worth remembering that whenever a record is made about someone they may one day access that information and with this in mind it is important to always use professional and courteous language.

Personal Data Breaches

A personal data breach will occur when personal data is lost, destroyed, corrupted or disclosed without proper authorisation. Some examples include:

- You accidentally leave some files containing patient personal data on the bus or train;
- You send an email or message containing patient personal data to the wrong patient;
- You accidentally delete a patient's records on an electronic system;
- Your email account is hacked and the hackers gain access to patient personal data.

A personal data breach will also occur where someone accesses personal data, or passes it on, without proper authorisation; or if the data is made unavailable, is accidentally lost or destroyed.

A personal data breach affects the confidentiality, integrity or availability of an individual's personal data. There are certain rules with respect to data breaches which, depending on the severity of the breach and the likely risk to the individuals concerned, may mean an obligation to report the breach to the ICO and in more serious cases may also mean reporting the breach to the affected individuals. Breaches must be reported without delay and there is a 72 hour time limit to do this which begins when the breach is discovered.

It is important that you are alert to data breaches and report them to the appropriate team as soon as you discover the breach. You should not report the breach to the ICO or affected individuals yourself unless you have been given appropriate training on this and this forms part of your role.

What should you be doing?

• Looking out for breaches and try to prevent them;
• Escalate – quickly!

If you notice anything suspicious such as an email that looks fraudulent (perhaps a hacker impersonating a colleague) or you realise that you have accidentally sent an email to the wrong person, or lost a hard copy file, or anything which you think has the potential to constitute a personal data breach – report it to the appropriate colleague or team as soon as you can.

Top Tips:

• Escalate – important that you are aware of your data protection obligations and prepared to spot issues and escalate them appropriately;
• Remember to use appropriate language whenever writing an email or making a written record or even a recorded phone call or voice note – the person you are writing about may one day see what you have written about them.
• Remember the principles:
• Lawfulness, fairness and transparency – would the individual expect you to do what you are doing with their data? Do they know about it?
• Purpose limitation – do you have a real purpose for processing data?
• Data minimisation – do you only collect the data you need?
• Accuracy – do you regularly check that the data you hold is accurate?
• Storage limitation – data cleansing
• Integrity and confidentiality (security) – lock your computers, drawers, offices
• Accountability – keep records of the decisions you have taken

For further information and guidance, please refer to the ICO's website - **ico.org.uk**

salts academy international