Understanding GDPR Workshop

Support Staff

GDPR – We know the rules – so how do we apply them in practice?

Let's test our knowledge… What are the 8 principles of data protection?

Fair & Lawful
Lawfully, fairly and in a transparent manner

Purposes
Specified, explicit and legitimate purposes (only those)

Adequacy
Adequate, relevant and limited to what is necessary

Accuracy
Accurate and, where necessary, kept up to date

Retention
Kept for no longer than is necessary

Rights Of Users
Gives individuals the right to choose how their personal data would be used

Security
Processed in a manner that ensures appropriate security

Data Transfer
Data should not be transferred outside the EU unless the country it is being transferred to can ensure adequate protection of the data

Subject Access Request

Patient's and customers are "data subjects" and have a right to access their patient records.

If a patient makes a subject data request what steps should you take to ensure the request is handled correctly?

Subject Access Request

Confirm Identity

Ensure the person you are talking to is the person that the data belongs to

Verify

Ask them to confirm 3 pieces of information such as name, DOB, address before providing information

Requests on behalf of the px

If someone is requesting on behalf of the px, ensure we have the px's consent to do so

Document

Record any requests or confirmations of consent on the px record to evidence that consent has been obtained

Scenario 1:

A patient comes in for a routine eye examination. The patient has been coming to the practice since childhood and is now 26. Since their last visit the patient now identifies as a female and will begin the process of gender reassignment soon.

The patient asks you to change their gender status on the records before going in for the eye examination. You advise the patient that the optometrist would have to change the records.

During the examination the patient advises the optometrist of the situation, as previously discussed with the receptionist. The Optometrist changes the patient's name on the record but not the title and gender. During the handover the Optometrist accidentally calls the patient Mr Smith.

After the dispensing process is completed the patient receives a text message a week later for "Mr Smith" advising to book a collection appointment.

Upon attending the collection appointment the patient is unhappy about the situation, and informs you that they want to make a formal complaint and requests that their records are deleted as they now wish to see an alternative eye care provider.

Discussion Points

- Does the patient have the right to change their gender details on their record and were you right in advising the optometrist can change it?
- How would you deal with the complaint?
- What type of information is the patient's gender & how should that information be handled?

"In 2004 the Gender Recognition Act was established and from then on permitted gender changes to be recognised lawfully/formally using a Gender Recognition Certificate (GRC). Official records, including medical records, cannot be changed without the patient presenting a GRC, where they have had their change in gender lawfully recognised. Only from then on, the new gender can be referred to legally in the records, from the date on the GRC."

"The right to erasure - This applies where there is no compelling reason for its continued processing. It is therefore not applicable where there is a duty to keep accurate records – e.g. keeping health and employee records is often a legal requirement or best practice and a requirement in case of a legal claim etc."

"The NHS specifies 7 years or, in the case of children under 18, until their 25th birthday. Accepted good practice in the profession is that records should be kept for 10 years after last contact with the patient"

Discussion Points

- Does the patient have the right to change their gender details on their record and were you right in advising the optometrist can change it?
- How would you deal with the complaint?
- What type of information is the patient's gender & how should that information be handled?

General Optical Council

"Operate a complaints system or follow the system that your employer has in place, making patients aware of their opportunities to complain to yourself or your employer. At the appropriate stage in the process, the patient should also be informed of their rights to complain to the General Optical Council or to seek mediation through the Optical Consumer Complaints Service."

"Provide any information that a complainant might need to progress a complaint, including your General Optical Council registration details and details of any registered specialty areas of practice."

Scenario 2:

A new receptionist starts today and receives a phone call from a patient who has an outstanding balance on their order and wants to make a payment over the phone.

Everyone is currently with a patient so the receptionist advises that they will take the details and get a colleague to process the payment and call the patient back to confirm it has been sorted.

The patient reads out their card details which are repeated back to them to confirm and then noted on a compliment slip with the patient's name, address and date of birth on before being handed over to a colleague to process.

The colleague who is handed the information puts it in their pocket before heading out to lunch and promises to process the payment on their return.

Discussion Points

- What should the receptionist have done differently?
- What potential breaches of GDPR have occurred?
- Who is responsible for the breaches of GDPR in this situation and how could they have been avoided?
- What should you do if you saw this happen?

General Optical Council

"Keep confidential all information about patients in compliance with the law, including information which is handwritten, digital, visual, audio or retained in your memory"

14. Maintain confidentiality and respect your patients' privacy

Discussion Points

- What should the receptionist have done differently?
- What potential breaches of GDPR have occurred?
- Who is responsible for the breaches of GDPR in this situation and how could they have been avoided?
- What should you do if you saw this happen?

"The Data Controller - Usually the practice or business owner or someone appointed by the practice or business owner who has overall control and responsibility for how personal data is collected, processed and stored in a practice/business."

Security

Processed in a manner that ensures appropriate security

"The data controller is responsible for determining how and why personal data is processed; responsible (and liable) for personal data and any breaches; responsible for reporting serious breaches and responsible for ensuring that data processors – people and organisations who handle data on the data controller's behalf - comply with the law"

Discussion Points

- What should the receptionist have done differently?
- What potential breaches of GDPR have occurred?
- Who is responsible for the breaches of GDPR in this situation and how could they have been avoided?
- What should you do if you saw this happen?

Optical practices are required to appoint a Data Protection Officer (DPO) if they provide GOS, or if they don't provide GOS but do process large amounts of special category personal data such as healthcare data. You should consider the following points carefully before deciding who to appoint as DPO:

- The DPO must have experience and expert knowledge of data protection law
- They should report directly to the highest level of management and have independence to perform their tasks
- Their other tasks or duties should not create a conflict of interest with their role as DPO

The tasks of a DPO are:

- To inform and advise the data controller and other staff about their obligations with regard to the GDPR and other data protection laws
- To monitor compliance with data protection laws and policies, raise awareness of issues and provide staff training
- To be the first point of contact with the ICO and for individuals whose personal data is processed.

Scenario 3:

A patient attends the practice for the first time for an eye examination. When registering you advise the patient that his contact details and personal data will only be used for the purpose of his eye care and is asked if he is happy to proceed, which he is.

The patient is unhappy with the final product when dispensed and requests a refund and a copy of his prescription with his PD measurement. The patient is given a copy of his prescription but not his PD measurement.

The patient then makes a formal request for his records and says he won't be coming back again..

The following year the patient is sent a reminder letter advising him that his eye examination is due, along with a separate email with information about a new range of spectacles that are being launched next week with a 20% off voucher.

Discussion Points

- Should you have given the patient his PD measurement on request?
- What potential GDPR breaches have occurred?
- If a breach of consent has occurred how should you deal with the situation?

“The PD measurement is not part of a prescription so doesn’t need to be documented on a copy, however, if you have recorded a PD measurement on the patient’s record then they do have a right to a copy of their records. The patient must make a formal data request which can be actioned in an appropriate time frame”

ABDO.

Discussion Points

- Should you have given the patient his PD measurement on request?
- What potential GDPR breaches have occurred?
- If a breach of consent has occurred how should you deal with the situation?

Practices and businesses will need to have at least one lawful basis for each processing activity.

“Consent should NOT be used as the lawful basis for health records, but is most likely to be the lawful basis when data is processed for marketing purposes.”

“Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject”

“Likely to be the lawful basis for health records for private patients and NHS patients treated through the NHS Standard Contract. May be used as the lawful basis for marketing to patients and others”

Discussion Points

- Should you have given the patient his PD measurement on request?
- What potential GDPR breaches have occurred?
- If a breach of consent has occurred how should you deal with the situation?

“A personal data breach is any breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

You do not have to report all breaches, but should learn from every event – e.g. near misses – in order to reduce future risks.

You have to report a data breach to the ICO where it is likely to result in a risk to the rights and freedoms of individuals, which if left unaddressed could cause a ‘significant detrimental effect’.

This includes breaches resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Data controllers will need to look at the facts and circumstances of each breach to decide what to do.

In the event of a serious breach the ICO must be notified within 72 hours without undue delay.”

Discussion Points

- Should you have given the patient his PD measurement on request?
- What potential GDPR breaches have occurred?
- If a breach of consent has occurred how should you deal with the situation?

Standard 19. Be candid when things have gone wrong

19.1 Be open and honest with your patients when you have identified that things have gone wrong with their treatment or care which has resulted in them suffering harm or distress or where there may be implications for future patient care.