General Data Protection Regulation – Briefing

NHS Midlands and Lancashire Commissioning Support Unit

1

Introduction

- Today's session is to give an overview of GDPR
- It is your responsibility to ensure GDPR compliance in your practice
- Further guidance is still coming out nationally from ICO, IG Alliance and NHS England

MIDLANDS AND LANCASHIRE COMMISSIONING SUPPORT UNIT 2

What is GDPR?

On the 25th May 2018 the Data Protection Act 1998 will be superseded by The General Data Protection Regulations (GDPR)

GDPR will become the new legislation on personal data

It will have some similarities to the previous DPA, however, there are new implications, deadlines and definitions

It is a living document and areas will be expanding with the UK implementing local adaptations

The UK's decision to leave the EU will not affect the commencement of the GDPR

There will also be a Data Protection Act 2018

MIDLANDS AND LANCASHIRE COMMISSIONING SUPPORT UNIT 3

What are the major changes?

- Fines are increasing – up to €20 million or 4% global annual turnover (whichever is the highest)
- Introduction of Data Protection Officer role
- Higher level of Accountability
- Consent – removal of implied consent

The 6 Principles of GDPR

New

The overarching Accountability Principle (Article 5(2)) requires that:
"The controller shall be responsible for, and be able to demonstrate, compliance with the principles"

1. Fair and lawful and transparent processing.
2. Obtained only for specified, explicit, legitimate and lawful purposes and not processed in an incompatible manner.
3. Adequate, relevant and limited to what is necessary
4. Accurate and up to date – every reasonable step taken to ensure inaccurate personal data is erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary
6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage

GDPR Accountability

The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility

In order to comply with this principle you must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply – such as policies, training for staff
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include: data minimisation, pseudonymisation, transparency, allowing individuals to monitor processing and creating and improving security features
- Use data protection impact assessments where appropriate

NHS
Midlands and Lancashire
Commissioning Support Unit

12 Steps to take now

7

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis for processing personal data
You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent
You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children
You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments
You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers
You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will fit in your organisation's structure and governance arrangements.

12 International
If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

ico. ico.org.uk

MIDLANDS AND LANCASHIRE COMMISSIONING SUPPORT UNIT 8

Step 1 - Awareness

Are your key people and decision makers aware of this change in Law? → What will the changes mean to your staff? → Organisational and personal liability

MIDLANDS AND LANCASHIRE COMMISSIONING SUPPORT UNIT 9

Step 2 - The Information You Hold

The GDPR covers *"Any information relating to an identified natural person (data subject). Can be identified directly or indirectly, in particular reference to an identifier such as name, id no., IP address, factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person"*

- How will we be certain we know what we hold and where it is held?
- Have you got all of your information assets into your asset register?

Step 3 - Communicating Privacy Information

- Fair processing notices will be known as a Privacy Notice
- It must be easy to understand and easily accessible
- Two click link to your privacy notice on your external website
- Maybe think about a layered approach

Step 4 - Individuals' rights

- Right to be Informed
- Right of Access
- Right to Rectification
- Right to Erasure**
- Right to Restrict Processing
- Right to Data Portability**
- Right to Object
- Rights Regarding Automated Decision Making and Profiling

Step 5 - Subject Access Requests

- Timescales are decreased – 40 days to 1 month
- Can no longer charge for access
- Team processes and standard operating procedures will be reviewed to ensure they remain relevant and fit for purpose

6. Legal Basis for Processing Personal Data

What is the legal basis for processing all the information that you do?	• Have you identified what information is held through an Information Audit and the Information assets recorded in your asset register
This links back to the rights of individuals	• If the processing is using consent as the legal basis then the data subject will have more rights

Has all of your processing been recorded onto you Fair Processing Notice?

Step 7 - Consent

How much of your processing of personal data relies on consent?

- Consent already obtained under the DPA will may be valid if it shows a clear affirmative action
- Data controllers must review all processing where consent has been used as the legal basis, to ensure they are compliant with GDPR
- Compliance must be achieved by 25th May 2018 or cease processing

Consent

Consent needs a clear affirmative act

- Freely given
- Specific
- Informed
- Unambiguous
- Must be demonstrable

Consent

Consent and medical matters

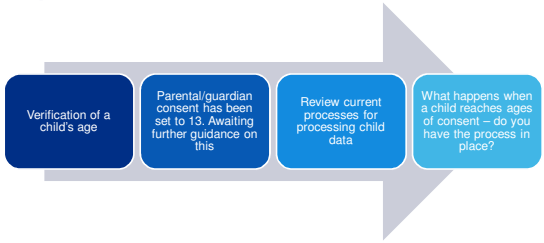
- "Consent should not be regarded as freely given if the subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment"
- Recital 42

Consent

Consent and confidentiality

- GDPR does not change the law of confidentiality
- Consent to override confidentiality may still be implied for direct care
- Caldicott 3 opt-outs still effective …
- **Provided** there is another GDPR basis e.g. "processing is necessary for the purpose of preventive medicine … medical diagnosis … the provision of health care and treatment … or the management of health systems and services … CCG duty to improve primary care services

Step 8 - Children



Step 9 - Data breaches

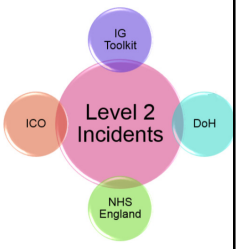
IG incidents and data breaches MUST be reported within 72 hours of being identified – awaiting further guidance on whether NHS will still remain with 24 hours

Lower tier fines up to 10 million Euros or 2% of global annual turner for not reporting data breaches

Identify current incident reporting processes

Incident reporting process
- *Included within the IG Handbook*

When to notify the data subject



Step 10 - Data Protection by Design & Data Protection Impact Assessments

Data Protection Impact Assessments will become a legal requirement	• This means you will need to have robust procedures
Data Protection by Design	• Having GDPR built into all processes and procedures
Privacy Impact Assessments	• To be renamed DPIA
High Risk Processing	• ICO Approval

Step 11 - Data Protection Officers

NHS organisations will need to appoint a Data Protection Officer (DPO) which can be someone internally, or externally

The DPO's minimum tasks are set out as:

- ✓Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- ✓Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- ✓Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)

Step 12 - International

Data Sharing Agreements

Review data flows

Is your data processed by another organisation outside of the EEA?

Review systems and software

Thank You for Listening

Any more questions?