NEL Commissioning Support Unit

NHS

The General Data Protection Regulation (GDPR) GP Awareness Session

Agenda

First Half

- Background
- Key Developments
- Headline Changes
- Application to Health
- Lawful Basis to Process
- Data Protection Impact Assessments
- Information Asset Registers
- Transparency
- Rights of Data Subjects
- Data Protection Officer

Second Half

- ICO 12 Steps to Compliance
- Resources
- Q&A

Background

- Enforcement date 25th May 2018
- Enforced irrespective of Brexit – Government, ICO and set out within the Queen's speech. Once enacted the UK will have the Data Protection Act 2018.
- This regulation – directly applicable. It is a MUST not a SHOULD.
- Some flexibility for member states to enact domestic legislation.
- Data Protection Bill will also come into effect, the Data Protection Act 1998 will be replaced with the DPA 2018
- Department for Culture Media and Sport leading on this - in particular to ensure business continuity by ensuring that essential current provisions still apply
- NHS England is leading a working group to support implementation

NEL

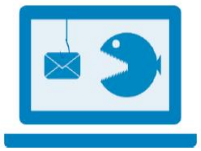
Ten Key Developments

Data Protection Officers

Explicit consent and lawfulness of processing

Data portability and access rights

Right to be forgotten

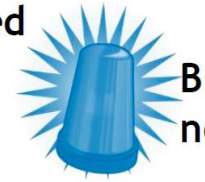


Data protection by design and default

Data transfers and the 'anti-FISA clause'

Freedom of expression and journalism

Measures based on profiling



Breach notifications

Data Protection Impact Assessments

NEL

Headline Changes -1

- Organisations obliged *to demonstrate that they comply with the new law*
- Tougher fines and penalties for *any* breach of the Regulation – not just data breaches
- Legal requirement for security breach notification- must be reported to ICO within 72hours
- Removal of charges, in most cases, for providing copies of records to patients who request them – Subject Access Request
- Requirement to keep records of data processing activities

NEL

Headline Changes - 2

- Appointment of Data Protection Officer **mandatory** for all public authorities
- Data Protection Impact Assessment required for high risk processing
- Data protection issues must be addressed in all information processes
- Specific requirements for transparency and fair processing – Accessible and in plain language
- Tighter rules where consent is the basis for processing. E.g. Automated decisions & Risk Stratification It as to be in writing.

NEL

Applicable to Health (and Care)

- As the with the DPA, the GDPR sets out conditions for lawful processing, and for processing 'special categories'
- 'legitimate interests' not available to public authorities – however there are other conditions that can be used – Public Task, Medical reason etc
- Social care is included with health as a condition for processing 'special categories'
- Criminal convictions data is not a special category

NEL

Ensuring a Lawful Basis

- Just like the Data Protection Act 1998, GDPR will require a lawful basis to process personal data and special categories of personal data.
- Processing personal data will require a condition in Article 6
- Processing special categories of personal data will require a condition in Article 6 and Article 9

Medical Purposes use

The most common use of (special category) personal data within a GP Practice will be for medical purposes.

The relevant Article 6 condition will therefore be Article 6(1)(e) *'…necessary in the performance of task carried out in the public interest or in the exercise of official authority…'*

Article 9(2)(h) can then be used to meet the requirements of medical purposes. This states:

*'processing is **necessary** for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems** and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

Other lawful basis

Other lawful basis available for non-medical related purposes:

- *Social Protection Law (Safeguarding)*
- *Vital Interests*
- *Substantial public interest*
- *Public health*
- *Defence of a legal claim*
- *Explicit consent*

Consent

- As with the DPA consent is one condition, with ‘explicit consent’ a condition for special categories
- As ‘*Consent should not be regarded as freely given if the data subject* ***has no genuine or free choice*** *…’* consent to data processing attached to consent to examination or treatment is unlikely to be valid
- However there are other options as above

GDPR, consent and the common law

- ‘implied consent’ better termed ‘reasonable expectation’ is not valid for GDPR (or now under DPA)
- However the GDPR does not invalidate the practice for common law purposes
- The principle of the Gillick competences applicable to children is unaffected, the default age will be reduced to 13 years.
- The GDPR helps here as the exacting requirements for transparency if implemented properly will support legitimate expectation

NEL

Data protection by design and default

- Technical and organisational measures to ensure compliance with the data protection principles in both the design and operation of data processing activities
- Such measures to include appropriate policies and the use of e.g. pseudonymisation
- Must ensure that only personal data that is necessary for each specific purpose of processing is processed

NEL

Information Asset and Data Flow Mapping

- Article 30 – Records of Processing
- Name of Data Controller, Data Processor and contact details of the Data Protection Officer
- Purposes of Processing
- Categories of Personal Data and Data Subjects
- Retention
- Technical and organisational security measures
- Processing on behalf of the Data Controller

NEL

Data protection impact assessment

Obligatory where:

- New technologies are to be introduced
- Processing is likely to result in a high risk to the rights and freedoms of data subjects
- Evaluation of personal aspects based on automated processing
- processing on a large scale of special categories of data (includes health and genetic data)
- systematic monitoring of a public area (CCTV, for example)

There is a list of essential elements of the DPIA.

- However, ‘a single assessment may address a set of similar processing operations that present similar high risks’
- After the impact assessment has taken place, in cases where the identified risks cannot be sufficiently addressed by the data controller (i.e. the residual risks remain high), the data controller must consult the ICO as per Article 36.

NEL

Transparency and fair processing

- information should be '…in a concise, transparent, intelligible, easily accessible form, using clear and plain language, in particular for any information addressed to a child…'
- Specific requirements for fair processing information e.g.:
  - the identity and contact details of the data controller or representative
  - contact details of the data protection officer
  - the purposes of processing and the legal basis (Articles 6 and 9)
  - where 'legitimate interests' applies, what these are (where Article 6(1)(f) applies – not available to public authorities)
  - recipients or categories of recipients
  - any intention to transfer data to a third country or international organisation, with information on adequacy and safeguards.
  - retention periods or criteria
  - existence of rights: access, rectification, erasure, restriction, to object, and portability….
  - existence of automated decision-making, logic, significance and consequences for the data subject.

NEL

Data Breaches

- Serious data breaches must be reported to the ICO in 72 hours
- GDPR states such breaches are those which would, or would be likely to:

"result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

- Fines can now up to €20,000,000 or up to 4% of annual turnover
- ICO have however stated that *'…it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm.'*

Data Subject's Rights

- Art. 15 - Right of access by the data subject
- Art. 16 - Right to rectification
- Art. 17 - Right to erasure ('right to be forgotten')
- Art. 18 - Right to restriction of processing
- Art. 20 - Right to data portability
- Art. 21 - Right to object
- Art. 22 - Automated individual decision-making, including profiling

NEL

Subject Access Requests

- Just as under DPA 1998, data subjects (e.g. patients and staff) will be able to request a copy of the information held about themselves
- Under GDPR, organisations cannot charge for providing this information
- There are certain exemptions, for example where information relates to another individual or is considered provided in confidence
- November 2016 – GP Practice fined £40,000 for disclosing information about a child and mothers location to the father of the child

NEL

Right to object

- Right to object ‘on grounds relating to his or her particular situation’
- Only available where processing is based on
  - 6(f)‘legitimate interests’ (not available to public authorities), or
  - 6(e)‘task carried out in the public interest or in the exercise of official authority vested in the controller’
- Processing of data under directions would not be subject to objection as 6(c) ‘ legal obligation’ applies

Right to prevent automatic decision making

- Right to object '…not to be subject to a decision based on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. '
- Doesn't apply where e.g.
  - Authorised by UK law which lays down safeguards
  - Based on explicit consent
- Where e.g. health data processed requires
  - Explicit consent or
  - Substantial public interest and safeguards
- Is likely to apply to risk stratification for case finding
- Applies to the decision not the profiling per se – although note right to object

NEL

The Data Protection Officer

- Obligatory for public authorities or where processing on a large scale or special categories data
- Must be independent (although they can be a member of staff or contractor)
- Must report to the highest management level of the organisation
- Must have 'expert knowledge of data protection law and practices, and the ability to perform the tasks specified in the GDPR:-
  - provision of advice to the organisation on compliance obligations, and when data protection impact assessment is required
  - monitoring compliance with the GDPR and organisational policies
  - co-operating and liaising with the Information Commissioner
  - taking into account information risk when performing the above

NEL

Data Protection Officers

- MDU: ‘The appointment of a data protection officer (DPO) will be mandatory for public authorities which include NHS primary medical and dental care practices. ’
- BMA: ‘All practices which provide services under an NHS contract are public authorities43 therefore it is mandatory that they designate, but not necessarily employ or retain, a DPO; a person with expert knowledge of data protection law’
- References in References slide

Pseudonymisation

- Pseudonymisation is given a statutory definition for the first time in the GDPR
- Circumstances in which pseudonymised data do not constitute personal data are likely to be limited.

Break

ICO 12 Steps to Take Now

- Awareness – Are Key Stakeholders aware?
- Information you hold (Information Asset Management)
- Communicating Privacy Notices
- Individuals Rights
- Subject Access Requests
- Lawful Basis for processing personal data
- Consent
- Children
- Data Breaches
- Data Protection Impact Assessments
- Data Protection Officers
- International

NEL

Resources

- Information Commissioners Office ‘Guide to the General Data Protection Regulation’
- (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/)
- Information Governance Alliance (NHS Digital) ‘GDPR: General Practitioner Advice Note’
  (https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance)
- British Medical Association ‘GPs as Data Controllers under the GDPR’
  (https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers)
- Medical Defence Union ‘Getting Ready for GDPR’
  (https://www.themdu.com/guidance-and-advice/guides/getting-ready-for-gdpr)


Questions