NEL Commissioning Support Unit

NHS

The General Data Protection Regulation (GDPR) GP Awareness Session Part II

Agenda

First Half

- Re-cap
- Developments since Part I
- Key Topics for Session
- Information Asset Register - Practical
- Data Protection Impact Assessments – Practical
- Rights of Data Subjects – Practical
- Data Protection Officer

Second Half

- 25th May - Where you Should Be
- Resources
- Q&A

Re-Cap

- Enforcement date 25th May 2018
- Implemented by new Data Protection Act 2018
- Makes current good practice mandatory under law
- Strengthens rights for citizens
- Introduces new requirement of mandatory data breach reporting (in certain circumstances)
- Need to appoint Data Protection Officer for GP Practices
- Increase in amount that can be fined – up to €20,000,000 or 4% of annual turnover

NEL

Ten Key Developments Since Part I

- Data Protection Bill still yet to achieve Royal Assent
- Currently at Consideration of Amendments stage
- GDPR will become law on 25th May regardless – there will be no national derogations

Key Topics

- Following from the first session, today will take a practical approach as opposed to the theory element before. This include a practical look at:
  - Information Asset Registers
  - Data Protection Impact Assessments
  - Rights of Data Subjects
  - Data Protection Officer

Information Asset Register

- Must include:
  - Name of Controller and Data Protection Officer
  - Purposes of Processing
  - Description of the categories of data subjects and personal data
  - Categories of recipients of whom the personal data will be shared with
  - Retention Schedules
  - Organisational and technical security measures
  - Lawful Basis
- How would the following assets be recorded?
  - Staff HR Records
  - Patient Electronic Records
  - Patient Paper Records

Rights of the Data Subject

- Rights of the Data Subjects are as follows:
  - Right of Access
  - Right to Rectification
  - Right to Erasure ('Right to be Forgotten')
  - Right to Restriction of Processing
  - Right to Data Portability
  - Right to Object
  - Right to no Automated-Decision Making
- Which apply to health records?

NEL

Rights of the Data Subject

- How would you respond to the following queries?
  - ‘Please could I have a copy of my medical record?’
  - ‘Please could I have a copy of my deceased fathers record?’
  - ‘Please could I have a copy of my son’s medical record?’
  - ‘Please could I have a copy of my employee file?’
- Each request should be handled on a case by case basis

Rights of the Data Subject

- How would you respond to the following queries?
  - ‘Under my right to be forgotten, please destroy my medical record’
  - ‘Under my right to be forgotten, please remove any mention of XX medication I have been taking’
  - ‘Under my right to object I request you not to share details of my condition with any other organisation including health services’
  - ‘Under my right to rectification I wish to have details of a conversation recorded on my record with my GP rectified to how I believe the conversation truly went’
- Each request should be handled on a case by case basis

Data Protection Impact Assessment

- GDPR requires that a DPIA is completed on all ‘high risk profiling’ or where special category data is used. As health data is considered special category it is likely that most new or changed methods of processing will require a DPIA
- Any new projects commissioned by CCG’s should have already had a DPIA completed on behalf of GP Practices
- However, as it’s likely that the GP Practice will be Controller for the personal data, you should request to see a copy of the DPIA to provide assurance that any risks have been identified and accepted or mitigated

Data Protection Impact Assessments

- If you are processing personal data in a new or different way which has not had CCG involvement you should ensure a DPIA has been completed. This will include:
  - Description of the personal data being processed
  - Purpose of processing
  - Description of the process
  - Parties involved in the processing
  - Legal basis for the personal data being processed
  - Assessment of necessity and proportionality of personal data being processed against the purpose
  - Assessment against rights and freedoms of individuals
  - Risks identified and appropriate measures documented

Data Protection Impact Assessment

- Think about the questions for these scenarios and complete a DPIA for these new/changed processes
  - You are purchasing a new HR system, moving away from storing these records on your shared drive
  - You are working with a third sector organisation who you will be sharing patient details with to help provide direct care to them
  - You are procuring text messaging software to help (a) send appointment reminders and (b) requesting to share mobile numbers with a third party supplier (such as a pharmaceutical company for marketing purposes)

NEL

Data Breaches

- Any data breach should be investigated and reported to the ICO in 72 if considered high risk. Things to consider when investigating a potential risk:
  - Data disclosed
  - Is it considered personal data or was it anonymised etc.
  - Number of individuals affected
  - If the personal data has been disclosed has it been recovered
  - If disclosed, was it disclosed to a closed environment or to the world at large
  - Was actual harm caused or was it potential harm
  - What are the consequences of the breach for the individuals involved?
  - What was the route cause of the breach?
  - What mitigations can be put in place to ensure such an incident doesn't happen again?

Data Breaches

- Consider these potential data breaches and carry out an investigation with the previous questions. Would you inform the ICO?
  - A father has requested a copy of his son's medical record (which he has a lawful basis to do so) but details of his ex wife have been included in the disclosure including allegations of domestic abuse against the father by the mother
  - A spreadsheet has been disclosed under a Freedom of Information request with the personal and medical details of 1000 patients has been disclosed in error on a tab that was hidden on the Excel document
  - An email providing information on an abortion support group has been accidently CC'd to 200 patients instead of BCC'd
  - A GP Practice has moved premises leaving historic paper patient records behind which have now ended up in the street after the property was broken into

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

Break

25th May - What to have in place

'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.'

'Those who self-report, who engage with us to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when we consider any regulatory action.'

Elizabeth Denham – Information Commissioner

NEL

25th May - What to have in place

Key Building Blocks according to the Information Commissioner:

- Organisational commitment – Preparation and compliance must be cross-organisational, starting with a commitment at board level. There needs to be a culture of transparency and accountability as to how you use personal data – recognising that the public has a right to know what's happening with their information.
- Understand the information you have – document what personal data you hold, where it came from and who you share it with. This will involve reviewing your contracts with third party processors to ensure they're fit for GDPR.
- Implement accountability measures – including appointing a data protection officer if necessary, considering lawful bases, reviewing privacy notices, designing and testing a data breach incident procedure that works for you and thinking about what new projects in the coming year could need a Data Protection Impact Assessment.
- Ensure appropriate security – you'll need continual rigour in identifying and taking appropriate steps to address security vulnerabilities and cyber risks
- Train Staff – Staff are your best defence and greatest potential weakness – regular and refresher training is a must

NEL

25th May - What to have in place

- On 25th May can you…
  - Demonstrate what information you hold and where it is and that you have a lawful basis to process it(Information Asset Management)
  - Demonstrate there is an understanding of the new changes within the organisation at all levels
  - Demonstrate the organisation is committed to compliance
  - Demonstrate you have appointed a Data Protection Officer
  - Demonstrate your commitment to transparency (privacy notices)
  - Demonstrate you have a process in place for completing DPIAs
  - Demonstrate you have a process in place for incident investigating and reporting
  - Demonstrate you have considered both physical security and cyber security
  - Demonstrate staff have undertaken training
- If you have yet to do part of this, can you demonstrate you have an action plan in place to meet these requirements?

NEL

25th May - What to have in place

- For each of the tasks, how would you rate your compliance on a scale of 1-5?
- Those tasks with lower scores across the board will be discussed to see if good practice can be shared across the Practices or a common approach taken to co-ordinate compliance

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