Northumberland, Tyne and Wear NHS Foundation Trust

Board of Directors Meeting

Meeting Date: 28 June 2017

Title and Author of Paper:
Awareness of the European General Data Protection Regulations (GDPR) Angela Faill, Head of IG and Medico Legal

Executive Lead: Lisa Quinn and Dr Rajesh Nadkarni

Paper for Debate, Decision or Information: Information

Key Points to Note:
Significant change Data Protection legislation - The European General Data Protection Regulations intends to strengthen and unify data protection within the European Union (EU). The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. The attached paper sets out a summary of the new/main changes. The key changes that will impact the Trust most are:

- Increased enforcement fines and data subject rights.
- Changes to the collection and recording of consent.
- Reduced timescales for processing subject access requests from 40 days to 30 days. This also covers access to health records.
- Individual rights to have information erased and corrected.
- Requirement for formal Data Protection Officer role.

Work is being done to manage the high impact changes and a detailed GDPR gap analysis and implementation plan is being developed.

Risks Highlighted: Financial & Reputational Risks are associated with non-compliance post implementation May 2018.

Does this affect any Board Assurance Framework/Corporate Risks:
Please state Yes or No – Not currently

Equal Opportunities, Legal and Other Implications: Legal Implications post implementation May 2018

Outcome Required / Recommendations: Trust Board members to be aware of the forthcoming changes and requirements and not actions to implement changes.

Link to Policies and Strategies: The GDPR will impact upon numerous national and local strategies and policies including IT, IG, Clinical/Corporate/Contractual arrangements and agreements.

Northumberland, Tyne and Wear NHS
NHS Foundation Trust

Awareness of the European General Data Protection Regulations

June 2017

Purpose

Trust Board members to note the contents of this paper.

Introduction

On 4th May 2016 the European General Data Protection Regulations (GDPR) – Regulation (EU) 2016/679 was passed.

With the General Data Protection Regulations, the European Commission intends to strengthen and unify data protection within the European Union (EU). As this is a European Regulation, it will have a direct effect and will not require domestic legislation to be passed. All EU member states will need to comply with the GDPR by the 25th May 2018.

Since Brexit seems unlikely to have effect until autumn 2018 at the earliest, it is probable that all UK organisations will need to comply with the GDPR for at least five months. This leaves organisations in a difficult position in terms of spending scarce resources. That said, it is highly likely that even after Brexit, the requirements of the GDPR will continue to apply in the UK. We therefore have little option but to prepare for the implementation of GDPR.

Much of the GDPR will be familiar territory to us in health. It builds on old concepts such as personal data and data controller, enhances existing rights and obligations and, in places, makes best practice a legal requirement.

Just one of the changes in relation to GDPR relates to fines. The maximum fine for non-compliance has risen from current financial penalties of around £500,000 to about £17 million at today's exchange rates. It is therefore of vital importance that the Trust gets this right.

Summary of the Main Changes

Enforcement

- The maximum fine for a breach has increased from £500,000 - £17 million (at today's exchange rate)
- It will become easier for data subjects to make a claim in relation to a data breach.
- Data Subjects will have the right to compensation from the data controller or data processor.

Accountability

- New principle of accountability means there is a need to demonstrate compliance. In this way, the Trust can be fined even if no 'harm' has occurred.
- The Trust must keep a record of processing through data flow mapping exercises.
- All new systems should be designed in accordance with privacy by design and privacy by default.

New Data Subject Rights

- Consent (for processing personal and personal sensitive data) must be freely given, specific, informed and unambiguous, provided by clear affirmative statement or action and which is able to be easily withdrawn.
- Parents will be required to provide their consent to the processing of children's personal data where those children are under a particular age (varying between 13 to 16 years old).
- The rules for dealing with subject access requests will change significantly under the GDPR:
  - The timeframe for the provision of the requested information is being reduced from 40 days to 30 days (it has been muted that this may be reduced further to 21 days).
  - There will be no more fees – with the removal of a fee there is an anticipated increase in request activity. (In 2016, NTW received 1,929 requests; there has been an increase in activity of 32% in the last 4 years.
- Individual Rights are strengthened in relation to:
  - having inaccuracies corrected;
  - having information erased;
  - preventing direct marketing;
  - preventing automated decision making and profiling, and data portability; and
  - having a wider right to be 'forgotten' than currently exists.

Data Protection Officers (DPO's)

All NHS bodies, LA and organisations whose core business is the delivery of health and social care must appoint a DPO. DPO's must be independent and must not be instructed on how to carry out his or her role within the organisation. DPO is a cornerstone of accountability and appointing a DPO can facilitate compliance. In addition to facilitating compliance through the implementation of accountability tools (such as facilitating or carrying out data protection impact assessments and audits), DPOs act as intermediaries between relevant stakeholders (e.g. supervisory authorities, data subjects, and business units within an organisation). DPOs are not personally responsible in case of non-compliance with the GDPR. Data protection compliance is a responsibility of the controller or the processor.

The DPO must report directly to the highest level of management (it has been suggested that they should report directly to the CEO)

Conditions for Processing

Stricter rules will apply to processing of sensitive personal data such as medical information. What constitutes sensitive personal data has been widened and will now include genetic and biometric data (i.e. any information which can identify who someone is).

Public Authorities can no longer rely upon the legitimate interests' condition BUT can rely upon carrying out a public function instead. The Schedule 3 medical purposes condition is expanded to expressly include social care and there is an entirely new Schedule 3 condition for public health, quality and safety of health care and quality and safety of drugs and medical devices.

Breach Notifications

- There is a new duty to inform data subjects of high risk breaches;
- There is a duty to notify Information Commissioner's Office (ICO) within 72 hours of breaches unless they are unlikely to result in a risk to the rights and freedoms of natural persons; and
- There is a duty to report to the ICO even if only small numbers of service users are affected.

New Duties for Data processors

- Duty under GDPR to for a data processor to act in accordance with controller instructions;
- Data processors become data controllers if they act beyond instruction;

- There are extra requirements for data processing requirements; and
- There will be restrictions on sub-contracting by data processors.

Fair Processing Notices

There is a requirement for extra information to be included in privacy notices, including data retention periods, source of data and an outline of the processing conditions relied upon.

Further, privacy notices need to be understood by children whose data is being processed by the organisation.

Best of the Rest

Privacy Impact Assessments (PIA) should be carried out as appropriate for all projects involving the processing of sensitive personal data on large scale. A privacy impact screening questionnaire will assess whether a PIA in necessary given the circumstances.

European Data Protection Board to replace Working party 29 with remit for guidance and consistent application of the GDPR

Conclusion and Recommendations

The Head of Information Governance and Medico Legal, supported by the Information Governance team are preparing for the implementation of GDPR by following the guidance published by the Information Commissioner. See Appendix 1 (attached).

The Head of Information Governance and Medico Legal will arrange specific GDPR/IG training for the Trust Board/Executive Officers and CDT (Senior Managers) in light of the new Information Governance landscapes.

The Head of Information Governance and Medico Legal is currently undertaking a gap analysis exercise by outlining the GDPR requirement/future state and comparing with the current Trust position.

An action plan will be developed outlining detailed actions needed to reach the GDPR requirement within the Trust.

The Head of Information Governance and Medico Legal to maintain a “watching brief” and provide regular updates during 2017 to the Trust Board, Executive Team and CDT and take direction on an ad hoc basis.

Appendix 1 - Information Commissioner's Office:

"Preparing for the General Data Protection Regulations (GDPR) – 12 steps to take now"

Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

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.

ico.org.uk

6 Legal basis for processing personal data

You should look at the various types of data processing you

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 sit within your organisation's structure and governance arrangements.

ico.
Information Commissioner's Office

carry out, identify your legal basis for carrying it out and document it.

International

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

Introduction

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which we expect to come into force in mid-2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. Over the next few months the ICO will set out its plans to produce new guidance and other tools to assist preparation. The Article 29 Working Party will also be producing guidance at European level. The ICO will also be working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about implementation in your sector.

It is essential to start planning your approach to GDPR compliance as early as you can and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Note that some parts of the GDPR will have more of an impact on some organisations than on others (for example the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

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 and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You should particularly use the first part of the GDPR's two-year lead-in period to raise awareness of the changes that are coming. You may find compliance difficult if you leave your preparations until the last minute.

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, across the organisation, or within particular business areas.

The GDPR updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

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.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your legal basis for processing the data,

your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. Note that the GDPR requires the information to be provided in concise, easy to understand and clear language.

The ICO is currently consulting on a new version of its Privacy notices code of practice. The new version, to be published later in 2016, will reflect the new requirements of the GDPR.

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.

The main rights for individuals under the GDPR will be:

- subject access,
- to have inaccuracies corrected,
- to have information erased,
- to prevent direct marketing,
- to prevent automated decision-making and profiling, and
- data portability.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. This is an enhanced form of subject access where you have to provide the data electronically and in a commonly used format. Many organisations will already provide the data in this way, but if you use paper print-outs or an unusual electronic format, now is a good time to revise your procedures and make any necessary changes.

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.

The rules for dealing with subject access requests will change under the GDPR. In most cases you will not be able to charge for complying with a request and normally you will have just a month to comply, rather than the current 40 days. There will be different grounds for refusing to comply with subject access request – manifestly unfounded or excessive requests can be charged for or refused. If you want to refuse a request, you will need to have policies and procedures in place to demonstrate why the request meets these criteria.

You will also need to provide some additional information to people making requests, such as your data retention periods and the right to have inaccurate data corrected. If your organisation handles a large number of access requests, the impact of the changes could be considerable so the logistical implications of having to deal with requests more quickly and provide additional information will need thinking through carefully. It could ultimately save your organisation a great deal of administrative cost if you can develop systems that allow people to access their information easily online. Organisations should consider conducting a cost/benefit analysis of providing online access.

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.

Many organisations will not have thought about their legal basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your legal basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your legal basis for processing.

You will also have to explain your legal basis for processing personal data in your privacy notice and when you answer a subject access request. The legal bases in the GDPR are broadly the same as those in the DPA so it should be possible to look at the various types of data processing you

carry out and to identify your legal basis for doing so. Again, you should document this in order to help you comply with the GDPR's 'accountability' requirements.

7 Consent

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

Like the DPA, the GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and unambiguous. Consent also has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes or inactivity. If you rely on individuals' consent to process their data, make sure it will meet the standards required by the GDPR. If not, alter your consent mechanisms or find an alternative to consent. Note that consent has to be verifiable and that individuals generally have stronger rights where you rely on consent to process their data.

The GDPR is clear that controllers must be able to demonstrate that consent was given. You should therefore review the systems you have for recording consent to ensure you have an effective audit trail.

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.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. In short, if your organisation collects information about children – in the UK this will probably be defined as anyone under 13 – then you will need a parent or guardian's consent in order to process their personal data lawfully. This could have significant implications if your organisation aims services at children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9 Data breaches

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

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. However, the GDPR will bring in a breach notification duty across the board. This will be new to many organisations. Not all breaches will have to be notified to the ICO – only ones where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach.

You should start now to make sure you have the right procedures in place to detect, report and investigate a personal data breach. This could involve assessing the types of data you hold and documenting which ones would fall within the notification requirement if there was a breach. In some cases you will have to notify the individuals whose data has been subject to the breach directly, for example where the breach might leave them open to financial loss. Larger organisations will need to develop policies and procedures for managing data breaches – whether at a central or local level. Note that a failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

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 (PIAs) and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management. You should start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

It has always been good practice to adopt a privacy by design approach and to carry out a privacy impact assessment as part of this. A privacy by design and data minimisation approach has always been an implicit requirement of the data protection principles. However, the GDPR will make this an express legal requirement.

Note that you do not always have to carry out a PIA – a PIA is required in high-risk situations, for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals. Note that where a PIA (or DPIA as the GDPR terms it) indicates high risk data processing, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

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 sit within your organisation's structure and governance arrangements.

The GDPR will require some organisations to designate a Data Protection Officer (DPO), for example public authorities or ones whose activities involve the regular and systematic monitoring of data subjects on a large scale. The important thing is to make sure that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively. Therefore you should consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements.

12 International

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

The GDPR contains quite complex arrangements for working out which data protection supervisory authority takes the lead when investigating a complaint with an international aspect, for example where a data processing operation affects people in a number of Member States. Put simply, the lead authority is determined according to where your organisation has its main administration or where decisions about data processing are made. In a traditional headquarters (branches model), this is easy to determine. It is more difficult for complex, multi-site companies where decisions about different processing activities are taken in different places. In case of uncertainty over which supervisory authority is the lead

for your organisation, it would be helpful for you to map out where your organisation makes its most significant decisions about data processing. This will help to determine your 'main establishment' and therefore your lead supervisory authority.