The Royal Wolverhampton
NHS Trust

General Data Protection Regulation and Cyber Security Declaration April 2018

Agenda Item No: 11.3

The Royal Wolverhampton NHS
NHS Trust

Trust Board Report

Meeting Date:	30th April 2018
Title:	General Data Protection Regulation and Cyber Security Declaration
Purpose of the Report:	To provide the Board with an update on the implementation of the General Data Protection Regulation 2016, Cyber Security and Data Security Protection Requirements.
Summary:	To provide an update on the Trust's progress on the implementation of the General Data Protection Regulation 2016. Data Protection Policy Statement for approval – to be available on Trust website in readiness for 25th May 2018. Data Security Protection Requirement- position statement on compliance with new assurance framework replacing the IG toolkit.
Action required:	To note the update report on GDPR for assurance. Approval of the Data Protection Policy statement – to be supported by a signature by the Caldicott Guardian, SIRO and Data Protection Officer. Approval of Data Security Protection Requirements for submission to NHS digital for 11th May 2018.
Clinical implications and view	N/A
Patient, carer, public impact and views	N/A
Resource implications	Role of the DPO and additional resources to support implementation of GDPR.
Report of:	Dr Jonathan Odum - Medical: Director/ Caldicott Guardian Kevin Stringer - Chief Financial Officer / Senior Information Risk Owner
Author + Contact Details:	Tel Raz Edwards – Information Governance Manager Tel 01902 307999 Email Raz.Edwards@nhs.net
CQC Domains	**Safe:** patients, staff and the public are protected from abuse and avoidable harm. **Effective:** care, treatment and support achieves good outcomes, helping people maintain quality of life and is based on the best available evidence. **Caring:** staff involve and treat everyone with compassion, kindness, dignity and respect. **Responsive:** services are organised so that they meet people's needs. **Well-led:** the leadership, management and governance of the organisation make sure it's providing high-quality care that's based around individual needs, that it encourages learning and innovation, and that it promotes an open and fair culture.

Trust Strategic Objectives	1. Create a culture of compassion, safety and quality 3. To have an effective and well integrated local health and care system that operates efficiently
Links to Assurances	
Resource Implications:	N/A
Equality and Diversity Impact	N/A
Risks:	N/A
Risk register reference:	N/A
Other formal bodies involved:	N/A
References	N/A

Report Details

1 **Purpose**

The GDPR comes into force across the EU on 25 May 2018 and will apply to the Trust as data controller, where we determine the purposes and means of processing personal data for both employees and patients, and also as data processors where we are responsible for processing personal data on behalf of another data controller.

The Trust has established a GDPR working group to address the changes and ensure compliance, with leads for specific work streams across various disciplines. This work is overseen by the Chair who is also the Trust Caldicott Guardian. The purpose of this report is to provide the Trust board with an update on the progression of the work streams as highlighted in Appendix A.

The report also details the GDPR/ data protection policy statement submission that is required before the 25th may 2018. Finally, the Data Security Protection Requirements that the Trust are required to review and sign off are also detailed below.

2 **Information Governance/ GDPR policy**

The Policy group has already had a meeting to discuss the re structure and the scale of the policy review (as demonstrated in appendix A). The IG/ GDPR policy was presented at the March policy Group. Due to the complexity of this area of law, resources and the fact that the Data Protection Bill has not been passed as an Act of Parliament, the group expressed concern with approving a policy at this stage. Instead it was agreed that a policy statement will be published supporting the minimum requirements that need to be communicated for the 25th May deadline, whilst a full policy review is continuing through the GDPR working group. The policy has been reviewed by the policy group members and GDPR working group members and is attached in appendix 2 for reference. This policy will require signature by Caldicott Guardian, SIRO and Data Protection Officer once approved by the board.

3 **Data Security Protection Requirements**

This year will see the instruction of a new IG toolkit now rebranded as the ‘Data Security Protection toolkit’.

	In January 2018, to improve data security and protection for health and care organisations the Department of Health and Social Care, NHS England and NHS Improvement published a set of 10 data and cyber security standards – the 17/18 Data Security Protection Requirements (2017/18 DSPR) – that all providers of health and care must comply with. The 2017/18 DSPR standards are based on those recommended by Dame Fiona Caldicott, the National Data Guardian (NDG) for health and care, and confirmed by government in July 2017. As part of the assurance process, the board must sign off the response before it is submitted. NHS improvement and NHS Digital have requested that all organisations subject to this toolkit submit a position statement to demonstrate their current position, championed by the Senior Information Risk Owner, approved by the Trust Board. This submission can be found in appendix 3.

Appendix 1

Key issue / GDPR Work stream	GDPR Implementation Group update	Next Actions	Timescales	Assurance level	Owner
1) Fair processing The right to be informed encompasses the obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how personal data is used.	Review of Trust wide privacy notice and communication methods to ensure compliance. Templates to be developed to assist specialists in publishing specific notices, once Trust notice has been agreed. Children specific notices are also now a legal requirement.	Trust Wide notice has been drafted and is being consulted on. This will be on the Trust website by the 25th May 2018. Service specific notice will follow thereafter.	July 2018		Head of Health Records
2) Rights of Access Individuals have the right to access their personal data and supplementary information with no free and within a shorter time scale (30 calendar days).The right of access allows individuals to be aware of and verify the lawfulness of the processing.	The Trust is currently assessing the impact the loss of income generated from subject access requests will have on performance within a shorter timescale. Anticipated increase in requests is also expected.	Review of OP07 to ensure new framework is reflected in current policy. SOPs and letters have been developed to support the process that will be in place for May 2018.	May 2018		Head of Health Records
3) Consent The GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance reputation. Consent requires a positive opt-in. No pre-ticked boxes or any other method of default consent.	The Trust needs to fully understand the GDPR consent guidance as it sets a much higher standard for consent. Currently lack of sector specific guidance in this area.	Development of a consent model to feature in review of OP07- Heath Records Policy. The Trust will need to assess processing where consent is used, and assess its appropriateness. A resource has been established for health records to carry out this	July 2018		Head of Health Records

		work and they will commence post in June.			
4) Breach reporting The GDPR introduces a duty on organisations to report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.	The Trust currently has a robust incident reporting system. This is being reviewed to ensure timescales and categories of incidents are consistent with new GDPR requirements.	Review changes to breach reporting categories for GDPR and update OP10 – Risk Management Policy but current process is compliant.	June 2018		IG Manager
5) Data processor - contacts and compliance Whenever a controller uses a processor it needs to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract.	Map out all arrangements with commercial providers undertaking data processing; identify where formal contractual agreements are in place. Approach providers to request their plans to comply with the regulatory obligations to ensure compliance.	GDPR assessment document for suppliers has been drafted and agreed. To be set to all suppliers where personal data is involved to assess compliance before end of May. Process will be established to assess responses between May and September.	March 2018		Head of Procurement
6) Privacy by design and Privacy Impact Assessments (PIA) Under the GDPR, the Trust is required to implement technical and organisational measures to show that we have considered and integrated data protection into processing activities.	New protocol to be written to include privacy by design when building/ procuring new systems for storing or accessing personal data. A new tool is being tested to support conducting privacy impact assessments.	Testing and roll out of PIA tool – as well as embedding its use into system and practice across Trust.	May 2018		Head of Projects and Assurance, IT

Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.					
7) Processing of children's data Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved. When processing children's personal data it should be demonstrated how the organisations aims to protect them from the outset, and design your systems and processes with this in mind. Clear privacy notices for children are also required so that they are able to understand what will happen to their personal data, and what rights they have.	The Trust is currently assessing processing relating to children's data to review what impact this requirement is likely to have.	A children's specific privacy notice is under development.	May 2018		Directorate Manager Children's services
8) Data portability The right to data portability allows individuals/ data subjects to obtain and reuse their personal data for their own purposes across different services. This only applies were data is provided with consent or under the performance of a contract.	The Trust is currently assessing the need to fully comply with this requirement, due to lack of guidance issued in this area. In the meantime options are being explored to facilitate the ability to move, copy or transfer personal data from one IT environment to another.	System owners contacted regarding data portability. Evaluating the potential for an in-house solution for the provision of data from clinical web portal.	May 2018		Head of Projects and Assurance, IT

9) Profiling and automated decision making The GDPR has specific provisions on: a) automated individual decision-making (making a decision solely by automated means without any human involvement; and b) Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process	The Trust currently assessing if and when this requirement would apply. Whilst such techniques may not be commonly utilised at present, it may become customary as technology and processing activities improve. At this stage the Trust is looking to establish a framework and model for this requirement.	Policy outline to be developed to satisfy the scope of this requirement.	June 2018		Information Manager
10) Mapping information assets and reviewing the basis for which we process.	The Trust has a comprehensive asset register which is being updated to be GDPR compliant. System owners are being established and risks/ legal basis for processing for each asset will be documented and reviewed. This will support compliance with the accountability principle of GDPR.	Detailed asset register in line with ICO guidance to be finalised and signed off.	May 2018		Head of Projects and Assurance, IT
11) Data subject rights, opt out, rectification, restriction. All rights available to data subjects should be communicated via fair processing notice and exercisable within 30 calendar days. • Right to be informed • Right to rectification	To review current policies to ensure it meets with GDPR regulation and add to OP07 and communicate to all staff. To publish 'rights' as part of the privacy notice.	Incorporate 'rights' into policy review OP07 – Health Records Policy and ensure there is clear process for communicating rights to data subjects.	May 2018		Head of Health Records

• Right of access • Right to erasure • Right to restrict processing • Right to data portability • Right to object • Rights relating to profiling and automated decision making					
12) Review data sharing agreements	A review of current data sharing agreements to ensure they are compliant and a review of the policy and templates to support future sharing.	Review of Wolverhampton overarching data sharing agreement, supporting policies and production of standard templates in line with GDPR. Tier 3 agreement has been ratified and is GDPR compliant. All new agreements will follow this template.	May 2018		IG Manager
13) Policy review Full review of IG related policies to streamline and update in light of legislative changes.	To review policy structure of IG and data protection policies to consider how to improve and streamline/ relaunch.	Policy statement has been approved and will be available on Trust website shortly. Other policies continue to be refreshed.	May 2018		IG Manager
14) Communication/ Training and Awareness Raise awareness to staff and the public around the GDPR, what it means and how the organisation is complying with this.	IG manager has already carried out a number of briefings for key staff. Trust wide training will be available in readiness for deadline.	Delivery of targeted training and briefing sessions. Trust wide e-learning has been developed and will be rolled out from May 2018.	May 2018		IG Manager
15) Accountability and governance and the role of the DPO	Identification of options for a statutory data protection officer. To clarify the role/ function of the	Finalising job description.	May 2018		Medical Director / Caldicott

The GDPR makes it a requirement that organisations appoint a data protection officer (DPO). The GDPR also contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO.	DPO. Communication of role an significance				Guardian
16) Pseudonymisation Processing personal data in such a way that data can no longer be attributed to a specific data subject without the use of additional information. This will allow organisations to utilise data whilst balancing the privacy of the data subject. GDPR sets out provisions in relation to this.	Whilst the Trust currently utilises such techniques, a formal process to be documented and governance of this is being considered.	New policy drafted and awaiting review by policy group in June – will sit under umbrella IG policy to detail the use of this technique.	June 2018.		Information Manager
17) Processing implications in relation to employee data The GDPR requires the same considerations to be given to employee data that is afforded to patient data. This includes privacy by design, communication of fair processing and rights of access.	Work is needed to understand the types of employee data that is processed and how this should be communicated more effectively to staff moving forward. Formal processes to be established to address this requirement for staff processing.	Policies for staff to be reviewed to incorporate changes in regulation. Fair processing notice is being drafted and will be communicated to staff before 25th May 2018. More work is needed to be done to support the rights available to staff, HR will look at the process that need to be in place to support this.	May 2018 for fair processing notice June for processes to support		Workforce manager

Appendix 2

1.0 Policy Statement: Data Protection Policy

The General Data Protection Regulation (GDPR) comes into force across the European Union on 25 May 2018 and will apply to the Trust as data controller, where we determine the purposes and means of processing personal data for both employees and patients, and also as data processors where we are responsible for processing personal data on behalf of another data controller. The below policy statement is designed to provide a high level declaration of the current position and the expectation in terms of compliance with the GDPR.

The GDPR represents a step change in the way that data is protected and managed and will be supplemented by the yet to be passed Data Protection Act 2018. GDPR introduces new rights for data subjects and strengthens existing rights available under previous laws.

The Trust has established a GDPR working group to address the changes and ensure compliance, with leads for specific work streams across various disciplines. This work is overseen by the chair who is also the Trust Caldicott Guardian.

This policy covers all aspects of information within the Trust, including but not limited to:

- Personnel information
- Patient/client/service user information
- Staff/ students/ trainee/ apprentices/ volunteers information
- Organisational information

1.1 Accountabilities

This Policy applies to the Trust and all its employees, whether they are on permanent, fixed term or temporary contracts, contractors, students and voluntary. It also applies to external contractors who are employed to carry out work on behalf of the Trust, whether this is a temporary or time limited capacity. 3rd parties will be notified of their duties in the terms and conditions of their contract. Each individual is responsible for ensuring that they comply with relevant legislation and guidance for protecting the data they use.

2.0 Legal basis for processing data

As a data controller the Trust must establish and publish the lawful basis that is relied on for processing personal data and data that is special categories (sensitive data). The following table indicates for the main processing legal basis that the Trust is relying on for processing activities. Every service processing personal or special category data must ensure they document (via an asset register) and communicate (via a fair processing notice – see section 4.1 Transparency below) which lawful basis they are relying to process data.

The GDPR sets out conditions for lawful processing of personal data (Article 6) and further conditions for processing special categories of personal data (Article 9) as listed in the table. If you are processing data relating to criminal convictions an Article 10 provision must also be satisfied.

3.0 Consent (Explicit consent)

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance reputation.

The GDPR definition of consent in Article 4(11) requires that:

- Consent must be given by a statement or by a clear affirmative action, and
- Consent must be freely given, specific, informed and unambiguous.

Only where there is no valid lawful basis to process data under GDPR then, individual's consent must be sought. Consent should not be used if a valid lawful basis exists.

Whilst consent may not be relied on for processing, there is still a requirement to inform the individual about how their data is being used (see section 4.1 transparency).

3.1 Consent and the Common Law (Implied consent)

If consent is not required under GDPR because another lawful basis exists, consent is still necessary to comply with the requirement of common law duty of confidence (confidentiality).

Implied consent is not a satisfactory standard for data protection law, as explained in section (3.0) as it must be an explicit clear affirmative action.

However for the purposes of common law, implied consent may be relied upon. This is consent which is not expressly granted by a person, but rather implicitly granted by a person's actions and the facts and circumstances of a particular situation – such as attending the emergency department or a GP.

Where consent is used to allow the lawful processing under GDPR, the following controls and considerations MUST be put in place:

- The requirement to facilitate withdrawal of consent – it must be as easy to withdraw as to give consent. This is known as Opt Out.
- The requirement that the Trust must be able to demonstrate that consent has been obtained. Consider where consent is recorded and ensure consent is dated so it is understood when it was obtained.
- the availability of the following rights (see rights in section 4.0):
- the right to erasure (where the subject withdraws consent and there is no overriding legitimate grounds to continue processing the data)
- The right to data portability.

3.2 Expiry of consent

In general once an individual has given consent, that consent may remain valid for an indefinite duration, unless the individual subsequently withdraws that consent. For the purpose of this policy the consent duration should be time limited to the specific 'piece of work' that is being proposed. It should be considered good practice to seek 'fresh' consent once the original piece of work is completed or there are significant changes in the circumstances of the individual or the work being undertaken.

3.3 Refusal and withdrawal of consent

If an individual makes a voluntary and informed decision to refuse consent for their personal information to be shared, this decision must be respected unless there are sound legal grounds for not doing so. An individual, having given their consent, is entitled at any time to subsequently withdraw that consent. Like refusals, their wishes must be respected unless there are sound legal grounds for not doing so. If an individual refuses or withdraws consent the consequences of doing so should be explained to them but care must be exercised not to place the person under any undue pressure.

4.0 Data Subject/ Individual Rights in relation to information

All rights that are listed below must be actioned within one month, unless stated otherwise. This can be extended by two months where the request is complex. A fee cannot be charged for processing of the request unless stated otherwise in this policy or supporting polices.

A request can be received both verbally and in writing so processes must be in place to ensure request can be logged and processed within the stipulated timeframes, please follow links below to local polices for how this applies in practice.

4.1 Transparency and the 'Right to be informed' – privacy notice

Individuals have the right to be informed about the collection and use of their personal data. The right to be told is also commonly referred to as a fair processing or privacy notice and is one of the most important rights. Regardless of what other rights apply to processing, the right to be told is fundamental to all rights being assessable by an individual. Done correctly the 'right to be told' about how information relating to the data subject is processed, should facilitate the use of data rather than hinder is use.

4.1.1 Privacy Notice Content

The following information must be communicated in the form of a privacy notice:

- The name and contact details of the Trust
- The name and contact details of our representative (if applicable).
- The contact details of our data protection officer
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing, (see section 2.5).
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

4.1.2 When to communicate privacy notice information

This information must be provided to individuals at the time their personal data is collected. If personal data is obtained from other sources, such as another organisation, individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month.

Link to privacy notice.

4.2 Right of Access to Information

Individuals have the right to access their personal data and supplementary information such as audit data or Metadata (data about the data). The right of access allows individuals to be aware of and verify the lawfulness of the processing.

As a minimum a data subject can make a subject access request and is entitled to receive in full:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see section 4.1).

Information must be provided within one month of receipt free of charge. However, a 'reasonable fee' can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive. For more details on how to make a request and when these conditions apply refer to the following

4.3 Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Where the information in question has been disclosed to others, each recipient should be contacted to inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients

4.4 Right to Erasure

The right to erasure is also known as the 'right to be forgotten' introduces a right for individuals to have personal data erased. A request for erasure can be made verbally or in writing, therefore processes should be put in place to ensure both types of request can be logged and monitored. The right to erasure is not an absolute right and should only apply in the following circumstances:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed;
- consent was the lawful basis for holding the data, and the individual withdraws their consent;
- legitimate interests was the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the data is processed for direct marketing purposes and the individual objects to that processing;
- the personal data has been processed unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- comply with a legal obligation; or
- the personal data is being processed to offer information society services to a child.

4.5 Right to Restrict Processing

The right to restriction allows an individual to request the restriction or suppression of their personal data. This right is closely linked with the right to rectify and the right to object. The right to restrict the processing of their personal data is not an absolute right and should apply in the following circumstances:

- the individual contests the accuracy of their personal data and the accuracy is being verified by the trust;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- the personal data is no longer needed in line with retention but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under section and you are considering whether your legitimate grounds override those of the individual.

- When processing is restricted, the personal data can still be stored, but cannot be further used or processed.

Where an applicant has made a request to **rectify (4.3)** or **object (4.7)** to processing of their data, then the individual may have a right to restrict processing whilst these rights are being assessed, so they should be considered at the same time. As a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question

4.6 Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The process should allow for moving, copying or transfer of personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability is not an absolute right and only applies:

- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

Therefore for care purposes, where data is processed under a statutory legal basis, the right to data portability would not apply. However where data is processed under the performance of a contract, with the individuals consent or the processing involves automated means, this right should be facilitated.

4.7 Right to Object

The right to object to processing means that data should cease to be processed. Individuals have the right to object to processing of their data where:

- Processing is based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); See section 2.0 for legal basis for processing).
- It is used for direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics (this does not include statutory reporting).

4.8 Rights relating to Automated Decision Making and Profiling

This is the process of making a decision solely by automated means without any human involvement, usually via a computer algorithm or formula. Profiling is automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.

Examples of this include:

- Risk stratification of patients based on frequency if attendance
- A recruitment aptitude test which uses pre-programmed algorithms and criteria.

If any of these techniques are used the following must be complied with:

- Send individuals a link the privacy statement data has been indirectly.
- Explain how people can access details of the information used to create their profile.
- Tell individuals who provide their personal data how they can object to profiling, including profiling for marketing purposes.
- Have additional checks in place for profiling/automated decision-making systems to protect any vulnerable groups (including children).

- Only collect the minimum amount of data needed and have a clear retention policy for the profiles created

Staff must read this policy in conjunction with the existing IG policies that are available on the Trust Intranet page which will continue to apply until they have been updated.

Caldicott Guardian Signature

Dr. J Odum (Medical Director)

. . . . . .

Senior Information Risk Owner (SIRO) Signature

Kevin Stringer (Chief Financial Officer)

. . . . . .

Data Protection Officer Signature

TBC

. . . . . .

Appendix 3

Leadership obligation 1: People

1. Senior level responsibility

There must be a named senior executive responsible for data and cyber security in your organisation.

Ideally this person will also be your senior information risk owner (SIRO), and where applicable a member of your organisation's board.

Fully implemented	Partially implemented	Not implemented
The organisation has a named senior executive who reports to the board who is responsible for data and cyber security and this person is also the SIRO	The organisation has a named senior executive who reports to the board who is responsible for data and cyber security but this person is not the SIRO	The organisation does not have a named senior executive who is responsible for data and cyber security

Please provide the contact details of the named senior executive responsible for data and cyber security if they are in place.

Name	Kevin Stringer
Job title	Chief Financial Officer
Name of organisation	The Royal Wolverhampton NHS Trust
Email	Kevin.Stringer@nhs.net
Telephone number	01902 307999

2. Completing the Information Governance toolkit v14.1

By 31 March 2018 organisations are required to achieve at least level 2 on the Information Governance (IG) toolkit. More information about the IG toolkit v14.1 can be found here: www.igt.hscic.gov.uk/help.aspx

For more information on how to complete the toolkit, please refer to the guidance:

- NHS foundation trusts: acute trusts, mental health trusts, ambulance trusts, community health providers, commissioning support units, NHS England
- independent providers: nhs business partners, commercial third parties, secondary use organisations, hosted secondary use teams, any qualified providers − clinical and any qualified providers − non clinical.

NOTE: the new Data Security and Protection toolkit is being introduced for 2018/19. This will replace the current IG toolkit.

Fully implemented	Partially implemented	Not implemented
The organisation has completed the IG toolkit, submitted its results to NHS Digital and obtained either level 2 or 3.	The organisation has completed the IG toolkit and submitted its results to NHS Digital but has not attained level 2.	The organisation has not completed the IG toolkit and submitted the results to NHS Digital

3. Preparing for the introduction of the General Data Protection Regulation in May 2018

The beta version of the Data Security and Protection toolkit was released in February 2018 and will help organisations understand what actions they need to take to implement the General Data Protection Regulation (GDPR) which comes into effect in May 2018.

Detailed information about the implementation of the GDPR can be found in the implementation checklist produced by the Information Governance Alliance (https://digital.nhs.uk/information-governance- alliance/General-Data-Protection-Regulation-guidance)

Fully Implemented	Partially Implemented	Not Implemented
By May 2018, the organisation will have an approved plan to detail how it will achieve compliance with the GDPR. This will have board-level sponsorship and approval.	By May 2018, the organisation will have a plan that has been developed but not yet sponsored and approved at board level on how it will achieve compliance with the GDPR.	A plan has not been yetbeen developed.

4. Training staff

All staff must complete appropriate annual data security and protection training.

As per the IG toolkit, staff are defined as: all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation.

A new training programme has been introduced: https://www.e-lfh.org.uk/programmes/data- security-awareness/. This programme replaces the previous IG training whilst retaining key elements of it. More information about the previous IG training resources can be found at https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=431663506918390&lnv=1&cb=6fa0a573- a4df-45f3-8af1-5c5ff58cce87&artid=170&web=yes

Providers must ensure staff have completed either the new IG training tool or the previous IG training tool.

Fully implemented	Partially implemented	Not implemented
At least 95% of staff have completed either the previous IG training or the new training in the last twelve months.	At least 85% of staff have completed either the previous IG training or the new training in the last twelve months.	Less than 85% of staff have completed either the previous IG training or the new training

Leadership Obligation 2: Processes

5. Acting on CareCERT advisories

Organisations must:

- Identify a primary point of contact for your organisation to receive and co-ordinate your organisation's response to CareCERT advisories, and provide this information through CareCERT Collect
- act on CareCERT advisories where relevant to your organisation
- confirm within 48 hours that plans are in place to act on High Severity CareCERT advisories, and evidence this through CareCERT Collect

Fully implemented	Not implemented
The organisation has registered for CareCERT Collect	The organisation has not registered for CareCERT Collect

Yes	No	Not applicable
The organisation has plans in place for all CareCERT advisories up to 31/3/2018 that are applicable to the organization (**Note**: the plan could be that the board accepts the residual risk)	The organisation does not have plans in place for all are CERT advisories up to 31/3/2018 that are applicable to the organisation	The organisation has not registered for CareCERT Collect

Fully implemented	Partially implemented	Not implemented
The organisation has clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in place.	The organisation does not have clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in place, but is developing these processes	The organisation does not have clear processes in place that allow it to confirm within 48 hours of a High Severity CareCERT advisory being issued that a plan is in place, and these processes are not under development

Fully implemented	Partially implemented	Not implemented
The organisation has in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories.	The organisation does not have in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories, but is in the process of filling that role.	The organisation does not have in post a primary point of contact who is responsible for receiving and co-ordinating CareCERT advisories, and no plans are in place to fill that role.

6. Business continuity planning

Comprehensive business continuity plans must be in place to support the organisation's response to data and cyber security incidents.

Fully implemented	Partially implemented	Not implemented
The organisation has an agreed business continuity plan(s) for cyber security incidents in place. The plan(s) take into account the potential impact of any loss of services on external organisations in the health and care system.	The organisation is developing a business continuity plan(s) for data and cyber security incidents. The plan(s) will take into account the potential impact of any loss of services on external organisations in the health and care system.	The organisation does not have a continuity plan for data and cyber security incidents in place

If there is a business continuity plan in place has it been tested in 2017/18?

Yes	No
The business continuity plan for cyber security incidents in has been tested in 2017/18.	The business continuity plan for data and cyber security incidents has not been tested in 2017/18.

7. Reporting incidents

Staff across the organisation must report data security incidents and near misses, and incidents should be reported to CareCERT in line with reporting guidelines.

Incidents should be reported to CareCERT via carecert@nhsdigital.nhs.uk or 03003035222 if part of a national cyber incident response.

Fully implemented	Partially implemented	Not implemented
The organisation has a process or working procedure in place for staff to report data security incidents and near misses	The organisation is developing a process or working procedure for staff to report data security incidents and near misses	The organisation does not have a process or working procedure in place for staff to report data security incidents and near misses

Leadership obligation 3: Technology

8. Unsupported systems

Your organisation must:

- identify unsupported systems (including software, hardware and applications)
- have a plan in place by April 2018 to remove, replace or actively mitigate or manage the risks associated with unsupported systems.

NHS Digital's good practice guide on the management of unsupported systems is at: https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care.

Other guidance and general documents are on the main CareCERT website.

Fully implemented	Partially implemented	Not implemented
The organisation has reviewed all its systems and any unsupported systems have been identified and logged on the organisation's relevant risk register	The organisation has reviewed all its systems and any unsupported systems have been identified but not logged on the organisation's relevant risk register	The organisation has not reviewed its systems to identify any that are unsupported

For any unsupported systems identified, has the organisation developed a plan for how it will remove, replace or actively mitigate or manage the risks of unsupported systems. Organisations are not required to submit a plan as part of this data collection process but should be prepared to submit their plan to NHS Digital if requested.

Fully implemented	Not implemented
By May 2018 the organisation will have developed a plan to remove, replace or actively mitigate or manage the risks associated with unsupported systems	By May 2018 the organisation will not have a plan in place to remove, replace or actively mitigate or manage the risks associated with unsupported systems

9. On-site cyber and data security assessments

Your organisation must:

- have undertaken or have signed up to an on-site cyber and data security assessment by NHS Digital
- act on the outcome of that assessment, including any recommendations, and share the outcome of the assessment with your commissioner.

Fully implemented	Partially implemented	Not implemented
The organisation has undergone an NHS Digital on-site cyber and data security assessment	Prior to 31 March 2018 the organisation signed up to undergo an NHS Digital on-site cyber and data security assessment but has not yet	Prior to 30 March 2018 the organisation has not signed up to an NHS Digital on- site cyber and data security assessment

For organisations who have undergone an NHS Digital on-site cyber and data security assessment:

Fully implemented	Partially implemented	Not implemented
The organisation has an improvement plan in place on the basis of the findings of the assessment, and has shared the outcome with the relevant commissioner(s)	The organisation has an improvement plan in place on the basis of the findings of the assessment, but has not yet shared the outcome with the relevant commissioner(s)	The organisation does not yet have an improvement plan in place on the basis of the findings of the assessment, and has not yet shared the outcome with the relevant commissioner(s)

Please tell us if the organisation has used an external organisation to audit the organisation's data and cyber security risks. Please note there is no requirement to use an external organisation to audit data and cybersecurity risks.

Yes	No
The organisation has used an external vendor to audit the organisation's data and cyber security risks	The organisation has not used an external vendor to audit the organisation's data and cyber security risks

10. Checking Supplier Certification

Organisation should ensure that any supplier of critical IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification (suppliers may include other health and care organisations).

Depending on the nature and criticality of the service provided, certification might include:

- ISO/IEC 27001:2013 certification: supplier holds a current ISO/IEC27001:2013 certificate issued by a United Kingdom Accreditation Service (UKAS)-accredited certifying body and scoped to include all core activities required to support delivery of services to the organisation.
- Cyber Essentials (CE) certification: supplier holds a current CE certificate from an accredited CE certification body.
- Cyber Essentials Plus (CE+) certification: supplier holds a current CE+ certificate from an accredited CE+ Certification Body.

Digital Marketplace: supplier services are available through the UK Government Digital Marketplace under a current framework agreement.

- Other types of certification may also be applicable. Please refer to Cyber Security services

NHS Digital contracts for/supplies a number of IT systems and solutions in use by multiple

NHS organisations. Please note that NHS Digital ensures in each of its system procurements that appropriate data security certifications are in place from its suppliers.

Fully implemented	Partially implemented	Not implemented
The organisation has checked that the suppliers of all its IT systems have appropriate certification, and can evidence that all suppliers have such certification.	The organisation has checked that the suppliers of IT systems that relate to patient data, involve clinical care or identifiable data have appropriate certification, and can evidence that all suppliers have such certification.	The organisation has not checked whether its suppliers of IT systems have appropriate certification.

Appendix 4 – legal basis for processing			
Type of processing	**GDPR Article 6 Condition for personal data**	**GDPR Article 9 Condition for special categories (sensitive data)**	**Statutory basis or other relevant conditions**
Lawful basis for direct care and administrative purposes All health and adult social care providers are subject to the statutory duty to share information about a patient for their direct care. This would also include (a) preventive or occupational medicine, (b) the assessment of the working capacity of an employee, (c) medical diagnosis, (d) the provision of health care or treatment, (e) the provision of social care, or (f) the management of health care systems or services (g) waiting list management (h) performance against national targets (i) activity monitoring (j) local clinical audit	6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…' 6(1)(d) is available in life or death situations but should not be necessary for health or social care organisations to use in the performance of its tasks. This might apply in a situation where an organisation needs to act to prevent harm being caused by a patient or service user, to someone who has no relationship with the organisation.	NHS Trusts National Health Service and Community Care Act 1990 NHS England's powers to commission health services under the NHS Act 2006 or to delegate such powers 251B of the Health and Social Care Act 2012
Lawful basis for commissioning and planning purposes Most national and local flows of personal data in support of commissioning are established as collections by NHS Digital either centrally, or for local flows by its Data Services for Commissioners Regional Offices (DSCRO).	Where the collection or provision of data is a legal requirement, for example where NHS Digital is directed to collect specified data, and can require specified organisations to provide it, 6(1)(c) '…for compliance with a legal obligation…'	9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'	Commissioners may receive personal data in support of commissioning where confidentiality is set aside by provisions under the Control of Patient Information Regulations 2002, commonly known as 'section 251 support'. This support does not remove the need for GDPR compliance.

			The commissioning of individually tailored services, or for example the approval of individual funding requests should operate on the basis of consent for confidentiality purposes.	
Lawful basis for research	6(1)(f)'…legitimate interests…except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject…'	9(2)(j) '…scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or member State law which shall be proportionate…and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject …'	A pre-condition of applying Article 9(2)(j) is that the processing has a basis in UK (or EU) law. This basis will include compliance with the common law duty of confidence, the provisions of DPA18 that relate to research, statistical purposes etc. & other relevant legislation, for example section 251 support.	
Lawful basis for regulatory and public health functions Processing that is necessary for reasons of public interest in the area of public health, and is carried out (i) by or under the responsibility of a health professional, or (ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.	6(1)(c) '…necessary for compliance with a legal obligation…	9(2)(j) ' …necessary for reasons of public interest in the area of public health…or ensuring high standards of quality and safety of health care and of medicinal products or medical devices…	Health Protection (Notification) Regulations 2010 Public Health (Control of Disease) Act 1984, as amended by the Health and Social Care Act 2008	
Lawful basis for safeguarding	6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official	9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the	Children Acts 1989 and 2004, and the Care Act 2014	

	authority…'	controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law..'		
Lawful basis for employment purposes	6(1)(b) 'For the performance of a contract to which the 'individual' is a party' Or 6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment…social protection law in so far as it is authorised by Union or Member State law..'	Safeguarding Vulnerable Groups Act 2006 as a basis for Disclosure and Barring Service (DBS) checks and other processing of such data	