Bolton Clinical Commissioning Group

Data Protection by Design Compliance Checklist

Policy Number	**IG020**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**17th September 2020**
Last Review Date	**April 2020**
Next Review Date	**17th September 2022**
Policy Author	**IG Team**
Version Number	**1.1**

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	February 2019	GMSS IG Team	New Document
0.2	February 2019	IG Board	Approved
1.0	March 2019	CCG Chief Officer	Approved
1.1	April 2020	IG Team	Reviewed – No Changes

Analysis of Effect completed:	By: Mike Robinson	Date: 30 Sept 2013

Contents

1. Introduction 4
2. Definitions 5
3. Data Protection by Design / Default Compliance Checklist 5

1. Introduction

GDPR now requires that the CCG put in place relevant technical and organisational measures / processes to ensure the data protection principles are adhered to and also to safeguard individual rights. This is known as "data protection by design and by default." This principle applies organisationally and requires the CCG to take account of data protection considerations even before it is decided whether the processing is likely to result in a high risk or not to individuals (which is principally what a Data Protection Impact Assessment (DPIA) is aimed to address). Data Protection by Design is not just the completion of a Data Protection Impact Assessment it involves all the measures that can be taken to ensure that data is protected, secure and confidential from when the idea of using personal data is originally thought about.

Therefore, it is essential that CCG considers data protection issues as part of the design and implementation of any system, service, product and / or business practice. This involves processes such as:

- developing new IT systems, services, products and processes that involve processing personal data
- developing organisational policies, processes, business practices and / or strategies that have privacy implications
- physical design
- embarking on data sharing initiatives
- using personal data for new purposes or changing the way personal data is being used for an existing purpose

The CCG must consider the intended processing activity and the data protection risk that this may pose to individuals and mitigate this with measures to ensure compliance with the data protection principles and to protect individual rights. This will then assist in complying with data protection by design and this checklist can assist to provide evidence of this. To find out more about individual rights, please see the Individual Rights Procedure.

In addition, the CCG needs to ensure that when personal data processing is required, that only the necessary and minimal data is processed to achieve the specified purpose. This links to the data protection principles of data minimisation and also pseudonymisation. This is known as 'data protection by default.' The CCG must specify this dataset before processing starts (using a Data Protection Impact Assessment (DPIA)). Once the DPIA is approved, the CCG must be transparent and appropriately inform individuals (via the Privacy Notice techniques) and then CCG must only process data needed for the specified purpose. There must be checks in place to ensure this is so.

It is now a legal requirement with GDPR to adopt both data protection by design and default principles. (Article 25).

Article 25 (1)

'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

And, Article 25 (2) states,

'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'

In addition, Article 25 (3) states that if the CCG adhere to an approved certification under Article 42, the CCG can use this as one way of demonstrating compliance with the above requirements. The CCG is currently working towards compliance with the NHS Data Security and Protection Toolkit (DSPT) which encompasses the GDPR principles and the National Data Guardian Data Security Standards.

2. Definitions

Data Protection by Design

Companies / organisations are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection by design').

Data Protection by Default

By default, companies / organisations should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default personal data isn't made accessible to an indefinite number of persons ('data protection by default').

Data Protection Impact Assessment (DPIA)

This is a process (risk assessment / questionnaire) to help identify and minimise the data protection risks of a project. GDPR places a new obligation to do a DPIA when the processing is likely to result in a high risk to individual's rights and freedoms relating to their data. In cases where high risks are identified, the Information Commissioners Office (ICO) must be consulted. The CCG adopts DPIA's for all new or changes to processing activities where personal data is used to assess ad mitigate any potential information risks. They assist with identifying data protection by design and default measures to be implemented. For further information about DPIA's, please see the DPIA Guidance and DPIA Proforma.

Privacy Enhancing Technologies (PETs)

These are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security and empowering individuals. They link to privacy by design and therefore can assist you to comply with this on a technical level.

3. Data Protection by Design / Default Compliance Checklist

In order to assist with implementing a Data Protection by design and default methodology, a set of standardised "Data Protection by Design Compliance Checklist" questions as detailed below must be complied with as a minimum aswell as completing a Data Protection Impact Assessment. Some of these questions are taken from the ICO guidance provided on this topic. The questions can also be used to review services that are already "live" and up and running to check data protection by design compliance.

This list is not exhaustive as there is no 'one size fits all' method but this will help ensure that key data protection issues are considered from the start of any data processing activity to ensure that relevant policies (such as a pseudonymisation procedure) and measures can be implemented to meet this requirement. Some examples are:

- Minimising the processing of personal data where practical

- Pseudonymisation of personal data
- Ensuring transparency
- Enabling individuals to monitor processing
- Creating and improving security features

A. Data Protection Impact Assessment (DPIA)

The first thing to do when you are deciding to use personal data for any activity is to complete a Data Protection Impact Assessment. Please see the DPIA Proforma and Guidance Notes for further information.

Completing this is fundamental to demonstrate that data protection issues are considered at the design and implementation of systems, services, produces and business practices. They also address key topics of data protection by design and default in the areas of: stating the legal basis for the data processing, certification, use of sub-contractors / data processors / information flows (including any international transfers), use and type of technology to be used and the organisational and technical security measures to be deployed.

B. Compliance Checklist

In addition to completing a DPIA, complete the questions below to check your data protection by design and default status for your proposed and / or current data processing activity. If you wish to add more information, please type this underneath the 'Yes / No' response boxes.

Action / Question
Q1. Complete a Data Protection Impact Assessment (DPIA)?
Yes☐ No☐
Q2. Have you assessed all the potential risks (such as risks to individual rights / privacy – invasive events) and taken steps / plans in place to prevent harm to individuals?
Yes☐ No☐
Q3. Do you know what the legal basis is under GDPR and / or DPA 2018 for processing the personal data for your purpose?
Yes☐ No☐
Q4. Are you only processing the personal data that you need for your purpose(s) and not for any other purposes?
Yes☐ No☐
Q5. Can you confirm that personal data is automatically protected in any IT system, service, product and / or business practice so that individuals should not have to take any action to protection their privacy?
Yes☐ No☐
Q6. Have you updated the Privacy Notice for your processing activity and ensured that this provides the identity and contact information of those responsible for data protection in the CCG and for individuals to contact if they need to?
Yes☐ No☐

Action / Question
Q7. Have you adopted a 'plain language' policy for any public documents so that individuals can easily understand what the CCG are doing with their data for your specified purpose?
Yes☐ No☐
Q8. Have you provided individuals with tools (e.g. online access / information how to action individual rights) so they can determine how you are using personal data and to check data protection policies / processes are enforced?
Yes☐ No☐
Q9. If you are providing an IT system / webpage, do you offer strong privacy defaults, user friendly options / controls and respect user preferences
Yes☐ No☐ N/A☐
Q10. If you sub contract, do you ensure that you only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design?
Yes☐ No☐ N/A☐
Q11. When choosing a system supplier, do you ensure that that you only choose suppliers / designers / manufacturers that have strong data protection compliance? Article 28 of the GDPR specifies the considerations you must take when selecting a data processor.
Yes☐ No☐ N/A☐
Q13. Do you regularly undertake audits to ensure the right people have access to data and that the minimal amount of data is being processed for your purpose?
Yes☐ No☐
Q12. Do you use privacy- enhancing technologies (PET) to assist you in complying with data protection by design obligations?
Yes☐ No☐ N/A☐
Q13. If you are using pseudonymisation and / or anonymisation techniques, have you referred to the ICO Code of Practice "Anonymisation: managing data protection risk code of practice? https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
Yes☐ No☐ N/A☐