My medical record

University Hospital Southampton NHS
NHS Foundation Trust

UHS NHSFT Informatics Service Data Protection Impact Assessment (DPIA) for MyMR

Reviewed and updated January 2019

UHSdigital

1 PURPOSE OF THIS DOCUMENT

This document is an updated Data Protection Impact Assessment (DPIA) for the My Medical Record Personal Health Record (PHR)

2 INTRODUCTION

A privacy impact assessment (PIA) was completed for the University Hospital Southampton NHS Foundation Trust (UHS NHSFT) My Medical Record (MyMR) project during 2016 and 2017. The PIA was signed off by the University UHS NHSFT Caldicott Guardian, Information Governance Steering Group (IGSG), and the information Strategy Steering Group during May and June 2017. At the time that the PIA was developed it was acknowledged that they were a relatively new concept within health care and the NHS and as such there was little formal guidance available.

Subsequent to the approval and sign off of the PIA various interested parties have provided comments and suggestions for the further development of the MyMR PIA, these include comments from the Information Governance Alliance (IGA), NHS Digital (NHSD) and the South Central and West Commissioning Support Unit (SCWCSU).

The General Data Protection Regulation (GDPR) which come into force on 25 May 2018 makes changes to PIAs, most obviously changing the name from Privacy Impact Assessment (PIA) to Data Protection Impact Assessment (DPIA) and making more substantive changes to the contents.

Because of feedback from interested parties, the new GDPR requirements, the experience gained from operating the MyMR solution in a live environment and the further development of the MyMR service both in terms the clinical scope and NHS Trusts users, it is opportune to review and revise the PIA.

The approach, structure and content of this DPIA has relied on the GDPR itself (European Parliament & Council of Europe 2016) and guidance from the UK Information Commissioner's Office (ICO) (ICO 2014; ICO 2018a; ICO 2018b), the EU Article 29 Data Protection Working Party (Article 29 Working Party 2017), UHS NHSFT data protection office (UHS Data Protection Office 2018), the Information Governance Alliance (IGA 2015; IGA 2018).

3 MYMR BACKGROUND INFORMATION

The MyMR service is a personal health record (PHR) for patients/healthcare service users and medical professionals. It is used to support the provision of healthcare for several clinical conditions by a number of NHS organisations. The MyMR service stores and displays health records for patients/healthcare service users and the medical professionals providing their healthcare.

MyMR have been developed by UHS NHSFT in partnership with software provider Get Real Health since 2012, it is being used to support over 9,000 patients. There are plans to scale the service further throughout 2018/19 with many more NHS Trusts going live.

4 SCOPE OF THE DPIA

The GDPR guidance (Article 29 Working Party 2017, sec.III a) allow for a single DPIA to be used to assess multiple processing operations that are similar "in terms of nature, scope, context purpose and risk" (Article 29 Working Party 2017, p.7). MyMR supports multiple clinical conditions and is used by a number of NHS organisations. MyMR uses similar technology to collect the same sort of data for the same purposes for each clinical condition and NHS organisation, as a result it is appropriate and permissible under GDPR (Article 29 Working Party 2017, sec.III a) for a single DPIA to be used for all the MyMR clinical condition and NHS organisations.

Article 29 Working Party (2017, p.7) guidance states that a single DPIA may "be applicable to similar processing operations implemented by various data controllers." As MyMR is used by a number of NHS organisations who are the data controllers, and the processing operations are similar for all users it is appropriate and permissible under GDPR for this DPIA to be a reference DPIA and shared with the various NHS organisations that use MyMR.

5 THE NEED FOR A DPIA

The ICO, IGA, Article 29 Working Party and UHS NHSFT Data Protection Office (ICO 2014; ICO 2018a; ICO 2018b; IGA 2015; Article 29 Working Party 2017; UHS Data Protection Office 2018) provide approaches to screening and assessing data processing operations to determine if they require a DPIA due to their inherent high risk.

The GDPR (European Parliament & Council of Europe 2016; Article 29 Working Party 2017) and UK ICO (ICO 2018a) require a DPIA where special category data (such as health records) are processed, as the core functions of MyMR is to provide a PHR MyMR requires a DPIA and it is not necessary to further assess the need for a MyMR DPIA. It is worth noting that of the Article 29 Working Party's nine criteria for assessing whether processing operations require a DPIA MyMR meets four of them:

1. Sensitive data or data of a highly personal nature e.g. special category medical records,
2. Data processing on a large scale,
3. Data concerning vulnerable data subjects, and
4. Innovative use of applying new technological or organisational solutions.

6 DESCRIPTION OF THE PROCESSING

The MyMR service is a personal health record (PHR) for patients/healthcare service users and medical professionals. It stores and displays health records for patients/healthcare service users and the medical professionals providing their healthcare. It is used to support the provision of healthcare for several clinical conditions by a number of NHS organisations.

6.1 NHS ORGANISATIONS AND THE CLINICAL CONDITIONS SUPPORTED BY MyMR

MyMR is used to support UHSFT clinical teams and patients in a number of different ways. The differing implementations across the 20 live pathways can be broadly grouped in to the following three areas –

1) **Patient Co-Production**; patients completing information at the request of their clinical team from home.
2) **Demand Management**; reduction in face-to-face outpatient appointments in transferring the management of stable follow-up patients to MyMR
3) **Patient experience/outcome**; instances where there may not be an obvious efficiency based business case but direct improvements to patient care can be made

The pathways live at UHS (as at 21/09/2019) are as follows –

Inflammatory Bowel Disease, Prostate Cancer, Congenital Cardiology, Lymphoma, Ready Steady Go (paediatric to adult transition), surgical pre-assessment, Genetic rare disease, Genetic adult cancer, Cystic Fibrosis, Paediatric Cardiology, Paediatric Nephrology, Colorectal cancer, Neuro headaches, Young adult rheumatology, Multiple Sclerosis, Huntingdon's disease, Parkinson's diseases, Motor neurone disease, Epilepsy.

The risk stratified cancer follow-up pathway is also implemented at the following hospitals (correct as of 21/09/2019) –

Royal United Bath, Royal Cornwall, Dartford & Gravesham, St Helen's & Knowsley, Aintree, Royal Liverpool, Southport, Countess of Chester, Gloucester.

6.2 NATURE OF THE PROCESSING

6.2.1 The information in MyMR may include:

- Details about patients/healthcare service users, such as name, address, email, date of birth, occupation, marital status, gender, ethnic origin, religion, next of kin, GP contact details.
- Contacts with patients/healthcare service users such as appointments and home visits.
- Notes and reports about the patients'/healthcare service users' health.
- Details and records about the patients'/healthcare service users' treatment and care.
- Details of the future care the patients'/healthcare service users may need.
- Results of investigations such as x-rays, ultrasounds, blood and other laboratory test results.
- Relevant information from people who care for the patients'/healthcare service users' and know them well, such as health professionals and relatives.

A detailed information audit and data flow mapping for MyMR is available on request.

6.2.2 The patients'/healthcare service users' information in MyMR may come from the following sources:

- The patients/healthcare service users manually.
- The patients/healthcare service users via devices.
- Medical professionals supporting the patients'/healthcare service users' healthcare this could include:
    - Staff involved in the provision of care, such as doctors, nurses, pharmacists and therapists
- Healthcare systems supporting the patients'/healthcare service users' healthcare.

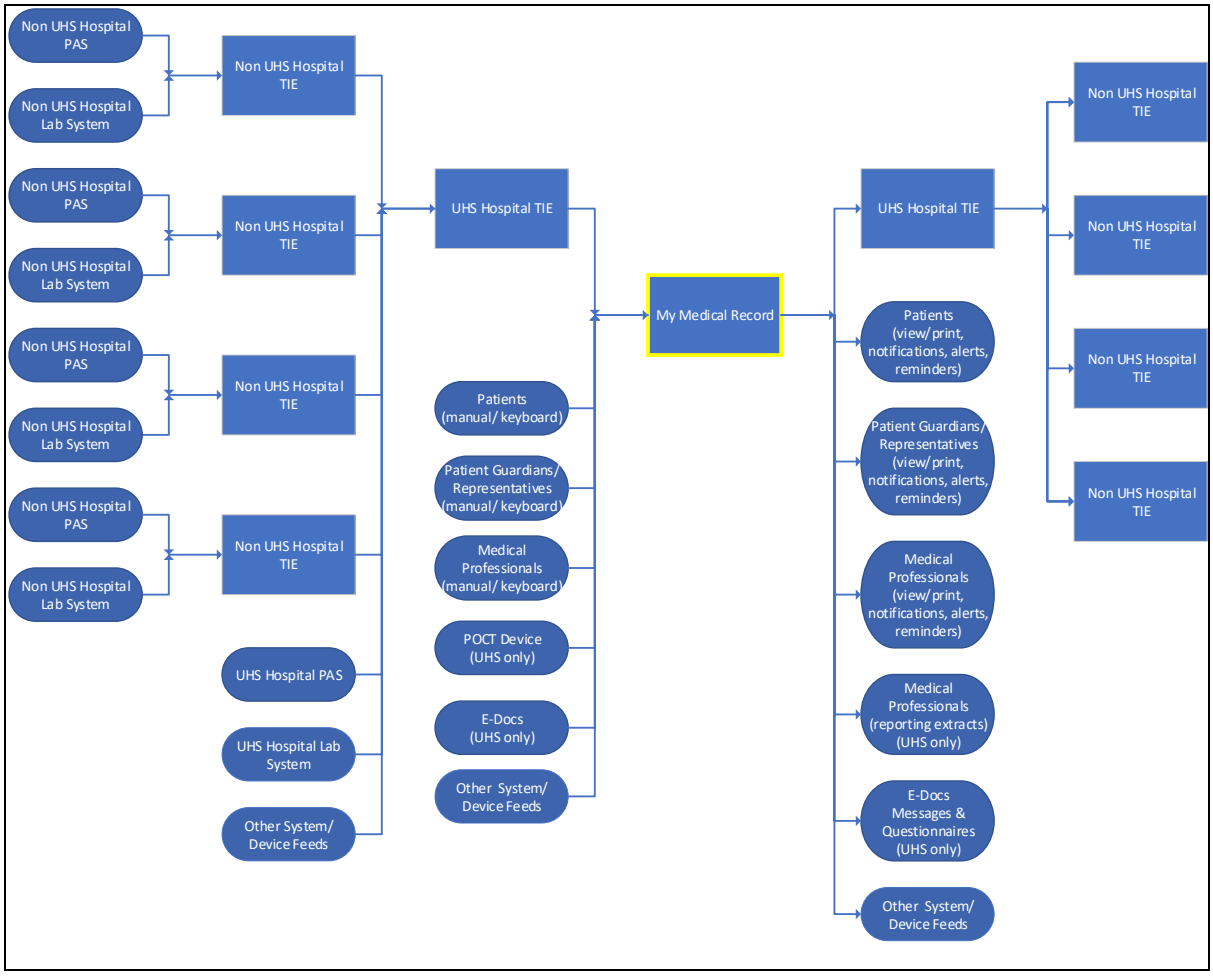
6.2.3 The patients'/healthcare service users' information in MyMR may be shared with:

- The patients/healthcare service users.
- Medical professionals supporting the patients'/healthcare service users' healthcare this could include:
    - Staff involved in the provision of care, such as doctors, nurses, pharmacists and therapists.
    - Staff involved in the administration of care, such as receptionists.
    - Healthcare students and professionals who are training.
    - Pathology and radiology staff who are analysing data.
    - Staff who are conducting local clinical audits.
    - Clinical research staff.
- Healthcare systems supporting the patients'/healthcare service users' healthcare.

6.2.4 High level data flow.

Figure 1 MyMR high level data flows shows the high-level data flow for MyMR.

Figure 1 MyMR high level data flows



6.2.5 How is the data stored?

UHS NHSFT host the MyMR service through the Microsoft Azure cloud-based platform. This approach supports the scaling of the service and results in benefits from the inherent security within Azure whilst also ensuring business continuity (e.g. protect against fail over, ensure appropriate capacity). The Azure instance that supports the MyMR service within a Microsoft data centre that is based in the UK. To support the MyMR service a dataset is stored within the UHS NHSFT network.

6.2.6 How long is the information retained?

As the MyMR service is one part of the provision of the patient/service user's overall healthcare the retention of the data is determined by the data controller as set out in their Privacy Notices and Records Management policy. It is worth highlighting that at present there are no national standards for data retention specific to PHRs, consequently general data retention policy of the data controller is applied to the MyMR service.

6.3 SCOPE OF THE PROCESSING

The categories of data processed by MyMR include: contact, demographic (including date of birth, gender, marital status and ethnicity), identification, and medical and health. The Medical and Health data includes the following sub categories: appointment, clinical messaging, general information, NHS identifiers, observation (description, date, time, result, unit), Holistic Needs Assessment questionnaires, patient monitoring questionnaires, Patient Reported Outcomes/Experience Measures questionnaires, personal & medical information questionnaires, consent questionnaires, medical record documents, reporting, test results auto – from a hospital lab system (description, date, time, result, unit, range), test result manual (input by the patient or clinician manually) and treatment schedules.

The personal information relating to health and medical, ethnic origin and sex life are special category data under the GDPR.

The geographical area covered by the MyMR data processing and the data subjects is nationwide across England and there are currently 13,798 (as at 21/01/2019) data subjects.

6.4 CONTEXT OF THE PROCESSING

The data subjects are NHS patients of UHS NHSFT or the other NHS organisations that use the MyMR service (see 6.1 for details of other NHS organisations using MyMR). It is reasonable to assume that the data subjects would expect the NHS organisations providing their healthcare to use a PHR to support the provision of healthcare.

Given the nature of the clinical conditions supported by MyMR, children and other vulnerable groups will be included within the data subjects.

The security of personal data and medical records is a high-profile topic within the NHS and wider society.

PHRs are relatively new and innovative, the technology is developing rapidly particularly in relation to data storage and remote access using cloud technology. In addition the automated linking of devices and wearable into an online PHR is an area that is likely to develop in the short to medium term. The devices and wearable could be clinical devices from the hospital or other healthcare provider (GP etc) or patients operating their own devices.

6.5 PURPOSE OF THE PROCESSING

Personal data is processed in MyMR to provide PHR which allow patients and healthcare service users to access their healthcare information. The medical professionals may use the MyMR service to support the provision of healthcare to patients'/healthcare service users'. The patients and healthcare service users' may be offered access to the MyMR service to help manage and support their healthcare.

7 CONSULTATION PROCESS

During the original development of MyMR key stakeholders were consulted to support the development of the solution and to support the assessment of the necessity and proportionality of the data processing and risk identification and mitigation. The stakeholders included medical professions, patients, the UHS NHSFT Caldicott Guardian, Information Governance Steering Group (IGSG), and the Information Strategy Steering Group (ISSG).

After the implementation of MyMR various interested parties and stakeholders have been consulted these include patients via patient day workshops, UHS Information Governance, the Information Governance Alliance (IGA), NHS Digital (NHSD) and the South Central and West Commissioning Support Unit (SCWCSU).

In late 2017 and May 2018 patients consulted via surveys, interviews, small group workshops and larger feedback sessions.

The UHS NHSFT Information Governance Manager has been consulted as part of the review and update to this DPIA and will review and sign off this updated DPIA along with the UHS NHSFT Data Protection Officer.

8 ASSESSMENT OF THE NECESSITY AND PROPORTIONALITY OF THE PROCESSING

8.1 LAWFUL BASIS FOR PROCESSING

The lawful basis for My Medical Record processing your data is:

> Article 6(1)(e) **Public task**: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

The clear basis is law for the public task lawful basis is derived from the various UK Government legislation that underpins the NHS these include:

- NHS Act 2006
- Health and Social Care Act 2012
- National Health Service and Community Care Act 1990
- Health and Social Care (Community Health and Standards) Act 2003

The special category condition for processing the data is:

> "Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, ***the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law*** or pursuant to

contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;"

8.2 Does the processing actually achieve the purpose?

Yes, since implementation MyMR has provided a PHR to support the provision of healthcare to NHS patients/healthcare service user by NHS medical professionals. The success of MyMR in achieving its purpose can be evidenced by its application to addition clinical conditions and its deployment by additional NHS organisations. An evaluation of the use of MyMR to enable the supported self-management of prostate cancer patients by five NHS organisations for c. 1,500 patients was positive.

8.3 Is there another way to achieve the same outcome?

There is no obvious suitable alternative to an untethered PHR such as MyMR.

8.4 How will function creep be avoided

The addition of new clinical conditions, NHS organisations and any material developments of the MyMR solution trigger a review of the DPIA by the UHS NHSFT Informatics team and the UHS NHSFT Information Governance Manager and Data Protection Officer.

8.5 How will data quality and data minimalization be ensured?

The original development of the MyMR solution adopted appropriate good practices, such as Data Protection by Design principles and the original PIA was signed off by the University UHS NHSFT Caldicott Guardian, Information Governance Steering Group (IGSG), and the information Strategy Steering Group.

The addition of new clinical conditions, NHS organisations and any material developments of the MyMR solution trigger a review of the DPIA by the UHS NHSFT Informatics team and the UHS NHSFT Information Governance Manager and Data Protection Officer.

8.6 What information will be provided to the data subjects?

MyMR has a GDPR compliant Privacy Notice which is available on the MyMR website/application and is linked to as part of the registration process.

8.7 How will data subjects' rights be supported?

The MyMR Privacy Notice sets out the data subjects rights and how to exercise them. Specifically, the Privacy Notice sets out the following data subject rights and how to exercise them:

- The right to be informed
- The right of access
- The right to rectification
- The right to restrict processing
- The right to object

- The right to lodge a complaint with a supervisory authority.

8.8 What measures will be taken to ensure data processors comply with GDPR?

UHS NHSFT Data Protection Office has taken steps to ensure UHS NHSFT data processors have GDPR compliant contracts in place. The UHS NHSFT Informatics team will actively manage relationships with any data processors to ensure GDPR compliance.

8.9 How are international transfers safeguarded?

MyMR does not currently transfer any data internationally and any plans to do so would constitute a material development of the solution and trigger a review of the DPIA by the UHS NHSFT Informatics team and the UHS NHSFT Information Governance Manager and Data Protection Officer.

9 Risk identification and mitigating activities

The Article 29 Working Party (2017) guidelines identify three high level risks to the rights and freedoms of data subjects that a DPIA should assess. These are:

- Illegitimate access.
- Undesired modification.
- Disappearance of data.

The ICO Sample DPIA Template (ICO 2018b), the ICO PIA code of practice (ICO 2014) and the IGA PIA guidance (IGA 2015) recommend the inclusion of the associated compliance and corporate risks that usually accompany data protection risks. For example, if a member of staff illegitimately accessed a celebrity patient's PHR this would be a data protection issue for the patient, a compliance issues as it is a breach of various data protection legislation, policies and procedures and a corporate issue as it is likely to results in fines, reputational damage and a loss of trust.

The compliance risks associated with most of the data protection risks in the DPIA relate to non-compliance with the Data Protection Act 2018 (DPA 2018), the GDPR, the Computer Misuse Act 1990 (CMA 1990) and various UHS NHSFT internal policies and procedures which include: the Information Governance Policy, the Policy for Use And Handling Of Patient Identifiable Data, the Informatics Security Policy, the Records Management Policy, and the Data Quality Policy.

The corporate risks associated with most of the data protection risks in the DPIA relate to Regulatory/ supervisory authority censure, enforcement action and/or fine, Reputational damage, Loss of public trust.

Table 9.1 is a summary of the identification, assessment and mitigating measures in relation to the main MyMR risks to individuals.

Table 9.1 MyMR DPIA risk identification, assessment & measures

MyMR DPIA risk identification, assessment & measures												
		Type	Gross Risk			Risk Response (TRAP)		Net Risk				
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
1	Malicious third party hack resulting in PHRs disclosed	Illegitimate access.	5	5	25	Reduce	Microsoft Azure cloud-based platform. Application of existing Trust procedures (info sec). DP by design. Information security good practice.	1	5	5	
2	Malicious third party hack resulting in PHRs altered	Undesired modification.	5	5	25	Reduce	Microsoft Azure cloud-based platform. Application of existing Trust procedures (info sec). DP by design. Information security good practice.	1	5	5	
3	Malicious third party hack resulting in PHRs deleted	Disappearance of data	5	5	25	Reduce	Microsoft Azure cloud-based platform. Application of existing Trust procedures (info sec). DP by design. Information security good practice.	1	5	5	
4	Staff member accessing a PHR inappropriately (e.g. friend, neighbour, family, celebrity)	Illegitimate access.	4	4	16	Reduce	Application of existing Trust training and procedures for DP training of staff. Access limited per clinical user to relevant	2	4	8	

MyMR DPIA risk identification, assessment & measures											
		Type	Gross Risk			Risk Response (TRAP)		Net Risk			
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
							patient cohort. System access audit trail				
5	Inadequate protection of the personal data of vulnerable patients, those with limited capacity and children who rely on a third party (parent/guardian/family member) to access their PHR	Illegitimate access.	4	4	16	Reduce	Application of existing Trust training procedures relating to access to vulnerable patients' data (e.g. records management etc). Access to the PHR determined by clinical staff applying existing safeguards resulting in not all patients given access to the PHR, delegate access only granted following appropriate governance checks	2	4	8	
6	Staff member amending information inaccurately	Undesired modification.	4	4	16	Reduce	Application of existing Trust training and procedures for quality. Staff training to reduce risk of unintended errors. System configured so only	2	3	6	

MyMR DPIA risk identification, assessment & measures											
		Type	Gross Risk			Risk Response (TRAP)		Net Risk			
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
							appropriate data can be deleted				
7	Staff member deleting information in error.	Disappearance of data	4	4	16	Reduce	Application of existing Trust training and procedures for quality. Staff training to reduce risk of unintended errors. System configured so only appropriate data can be deleted	2	3	6	
8	Loss of some data from MyMR due to technical failure	Disappearance of data	4	4	16	Reduce	Microsoft Azure cloud-based platform, built technical resilience. Secure data back up. Application of existing Trust procedures (info sec). DP by design. Information security good practice.	1	4	4	

MyMR DPIA risk identification, assessment & measures												
		Type	Gross Risk			Risk Response (TRAP)		Net Risk				
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
9	As a result of unauthorised disclosure of a patients PHR they are harmed physically or emotionally.	Illegitimate access.	3	5	15	Reduce	General security of the system (see above) to reduce the risk of third party access. Training and information to patients and users to reduce risk of unauthorised access (e.g. password management). Application of existing data protection and info security procedures to reduce risk of unauthorised disclosure of data.	2	5	10	
10	Loss of all data from MyMR due to technical failure	Disappearance of data	3	5	15	Reduce	Microsoft Azure cloud-based platform, built technical resilience. Secure data back up. Application of existing Trust procedures (info sec). DP by design. Information security good practice.	1	5	5	

MyMR DPIA risk identification, assessment & measures												
		Type	Gross Risk			Risk Response (TRAP)		Net Risk				
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
11	Patient entering/amending information inaccurately	Undesired modification.	4	3	12	Reduce	Dissemination of guidance for patients through various channels. Data input validation where appropriate. Audit trail of who input/amended which data. MyMR data not the primary source for clinical judgement	3	3	9	
12	Patient deleting information in error.	Disappearance of data	4	3	12	Reduce	Dissemination of guidance for patients through various channels. Data input validation where appropriate. Audit trail of who input/amended which data. MyMR data not the primary source for clinical judgement	3	3	9	

MyMR DPIA risk identification, assessment & measures											
		Type	Gross Risk			Risk Response (TRAP)		Net Risk			
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
13	As a result of unauthorised disclosure of a patients PHR they are discriminated against.	Illegitimate access.	3	4	12	Reduce	General security of the system (see above) to reduce the risk of third party access. Training and information to patients and users to reduce risk of unauthorised access (e.g. password management). Application of existing data protection and info security procedures to reduce risk of unauthorised disclosure of data.	2	4	8	
14	Incomplete medical information that could lead to clinical error.	Undesired modification.	3	3	9	Reduce	End to end testing of data feeds for accuracy. Clinicians rely on more than just data from MyMR when making clinical judgements.	3	2	6	
15	Inappropriate/unauthorised data sharing within and between NHS organisations	Illegitimate access.	3	3	9	Reduce	Appropriate sharing of MyMR data between UHSFT and other Trusts is handled within a signed SLA. Any material developments of the MyMR solution trigger a	2	3	6	

MyMR DPIA risk identification, assessment & measures											
		Type	Gross Risk			Risk Response (TRAP)		Net Risk			
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
							review of the DPIA by the UHS NHSFT Informatics team and the UHS NHSFT Information Governance Manager and Data Protection Officer.				
16	MyMR scope creep resulting in the purpose for processing patient data changing without appropriate approval or notification to data subjects.	Illegitimate access.	3	3	9	Reduce	Any material developments of the MyMR solution trigger a review of the DPIA by the UHS NHSFT Informatics team and the UHS NHSFT Information Governance Manager and Data Protection Officer.	2	3	6	
17	Patients not understanding what the MyMR PHR is and how or why their data is processed	Illegitimate access.	4	2	8	Reduce	Link to GDPR compliance Privacy Notice included as part of registration and available on the system. Updated 'About MyMR' section explains nature of the service	3	2	6	

MyMR DPIA risk identification, assessment & measures											
		Type	Gross Risk			Risk Response (TRAP)		Net Risk			
Ref	Description of Risk	Individuals	Likelihood (5=Very high)	Impact (5=Very high)	Overall Risk (LxI)	TRAP	Response	Likelihood	Impact	Overall Risk	Accepted
18	Staff accessing MyMR after leaving the organisation or department	Illegitimate access.	2	3	6	Reduce	Application of existing Trust procedures for staff access to IT systems when leaving or changing roles or departments. UHS Published leavers list is acted upon appropriately. Responsibiilty of other hospitals to inform UHS of any leavers	1	3	3	
19	Patient mis-match upon registration resulting in a single breach to a single record	Undesired modification.	3	1	3	Reduce	Re-developing registration process to improve data quality checks	2	1	2	

This risk assessment was developed from the original 2017 PIA risk assessment and management review. Feedback from key stakeholders (Data Protection team, Commissioning Support Unit, NHS Digital, patient and clinical users etc) on the original PIA's risk assessment has, where appropriate, been incorporated into the above assessment. It is intended that stakeholders will continue to be consulted on MyMR risk management.

10 DPIA REVIEW

MyMR continues to be deployed to additional NHS Trusts for the existing clinical conditions and being developed to support new clinical conditions. It is important that the DPIA is reviewed and updated to reflect the changes in which NHS organisations are using it and what clinical conditions are being supported. This review and update process will ensure the lawful basis and purpose of processing the data remain accurate, and that the types of data and data flows into and out of MyMR are up to date and appropriate.

This DPIA will be reviewed by the UHS NHSFT Informatics team and the UHS NHSFT Information Governance Manager and Data Protection Officer as follows:

- Full annual review
- Quarterly review to changes triggered by:
    - Material developments and significant changes to MyMR.
    - New clinical conditions
    - New Trusts
    - Material system upgrades

11 REFERENCES

Article 29 Working Party, 2017. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing in "likely to result in a high risk" for the purposes of the Regulation 2016/679*, Brussels.

European Parliament & Council of Europe, 2016. *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, European Union: European Parliament and Council of Europe.

ICO, 2014. Conducting privacy impact assessments code of practice. , pp.1–51.

ICO, 2018a. Guide to the General Data Protection Regulation (GDPR) v1.0.49. , pp.1–153.

ICO, 2018b. Sample DPIA template. , pp.1–7.

IGA, 2015. Privacy Impact Assessments. , pp.1–13.

IGA, 2018. *THE GENERAL DATA PROTECTION REGULATION: IMPLEMENTATION CHECKLIST*, London.

UHS Data Protection Office, 2018. Data Protection Impact Assessment. , pp.1–6.