DATA SHARING AGREEMENT WITH FAIRFIELD INDEPENDENT HOSPITAL AND WEST LANCASHIRE CLINICAL COMMISSIONING GROUP MAY 2018

Issue 1 Review

May 2018 May 2020

CONTENTS

1. Policy Statements and Purpose of this Data Sharing Agreement 3

2. Legal Basis for Data Sharing 3

3. Data 3

3.1 What data is it necessary to share? 4

3.2 Who is going to be responsible for sharing this data and ensuring data is accurate? 4

3.3 How will you keep a record of what data has been shared? 4

3.4 How is this data going to be shared? 4

3.5 Who will have access to this data and what may they use it for? 5

3.6 Timescales 5

3.7 How securely does the data need to be stored? 5

3.8 How long are you going to keep the data? 5

3.9 Further Use of Data 5

4. Breach of confidentiality 6

5. Complaints procedures 6

6. Access to Information 6

7. Indemnity 7

8. Review of Data Sharing Agreement 7

9. Closure/termination of agreement 8

10. Signatories 8

1. POLICY STATEMENTS AND PURPOSE OF THIS DATA SHARING AGREEMENT

Fairfield Independent Hospital wants to send all patients' information to the GP practices of West Lancashire via electronic means. This is to ensure it remains secure. The Hospital aim to send all patient information electronically to make it secure and to reduce postage costs. The patient information shared will be included in Patients letters and discharge letters. These will be sent through Docman or alternative means to the GP's in West Lancashire.

2. LEGAL BASIS FOR DATA SHARING

GDPR Article 6(1)(e) the 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.

This public task would fall under Section 3a of the NHS Act 2006 as amended by the Health and Social Care Act 2012:

> **Section 3A NHS Act 2006**
>
> Each CCG has the power to arrange for the provision of such services or facilities as it considers appropriate for the purposes of the health service that relate to securing improvement in –
>
> (a) The physical and mental health of persons for whom it has responsibility; or
>
> (b) The prevention, diagnosis and treatment of illness in those persons.

GDPR Article 9(h) processing necessary for the purposes of…..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.

3. DATA

3.1 WHAT DATA IS IT NECESSARY TO SHARE?

The patient's identifiable data stipulated on the patient's letters and correspondence is their Date of Birth, NHS Number and Fairfield Hospital number.

Data Set	From Fairfield Independent Hospital	To GP's in West Lancashire	Which Organisation owns the information (Who is the Data Controller?)	Frequency of Sharing
Name	Yes	Yes	FIH & GP's	Daily
D.O.B	Yes	Yes	FIH & GP's	Daily
NHS Number	Yes	Yes	FIH & GP's	Daily

3.2 WHO IS GOING TO BE RESPONSIBLE FOR SHARING THIS DATA AND ENSURING DATA IS ACCURATE?

All information sent to the GP Practices on discharge reports will be checked by senior members of staff on the wards. Medical Secretaries will be responsible for checking all letters for accuracy, under the management of the CEO. X-ray reports will be checked by the Radiographers.

Fairfield Independent Hospital are currently using Docman to process this data. This means that Fairfield Independent Hospital will require access to the system in use by the GPs of West Lancashire.

3.3 HOW WILL YOU KEEP A RECORD OF WHAT DATA HAS BEEN SHARED?

The data will be logged electronically on the systems used by both Fairfield Independent Hospital and the GPs of West Lancashire.

3.4 HOW IS THIS DATA GOING TO BE SHARED?

The data will be shared via Docman.

3.5 WHO WILL HAVE ACCESS TO THIS DATA AND WHAT MAY THEY USE IT FOR?

X-ray staff will have access for sending X-ray reports. Medical Secretaries will have access for sending letters to GPs and Ward Staff will have access to issue discharge reports.

3.6 TIMESCALES

Information will be shared on a daily basis as per the table in 3.1

3.7 HOW SECURELY DOES THE DATA NEED TO BE STORED?

CCG's to advise on the method of transporting data and Fairfield Independent Hospital can then draw up procedures and implement them with their teams. Risk assessments will be completed and the process will be embedded into ISO 27001.

If there is a security breach in which data received from another party under this agreement is compromised, the originator will be notified at the earliest opportunity via the post holder identified at 3.2. as per Fairfield Independent Hospitals breach management procedures.

For further information please refer to the Privacy Impact Assessment (Appendix 1).

3.8 HOW LONG ARE YOU GOING TO KEEP THE DATA?

Destruction of records will be completed in line with Fairfield Independent Hospital Destruction of Records Policy which adheres to the NHSE Records Management Code of Practice.

3.9 FURTHER USE OF DATA

There are no plans for further use of data beyond those stated in section 1.

4. BREACH OF CONFIDENTIALITY

The severity of the incident will be determined by the scale (numbers of data subjects affected) and sensitivity factors selected. If the outcome in terms of the severity of the incident is IG SIRI level 2 (reportable) an email notification will be sent to the HSCIC External IG Delivery Team, DH, ICO and escalated to other regulators, as appropriate (pure Cyber SIRI notification Department of Health (DH) and HSCIC only). If the outcome is IG SIRI level 0 or 1 no notifications will be sent.

Wherever possible, incidents will be logged and notified on the IG Incident Reporting Tool as soon as possible once the organisation becomes aware of the data breach (usually within 24 hours).

As per the requirements of the General Data Protection Regulation. Any breaches that are likely to result in a high risk of adversely affecting individuals' rights and freedoms will be notified to the Information Commissioners Office within 72 hours (where feasible) and data subjects will be informed of the breach regarding their personal data.

5. COMPLAINTS PROCEDURES

The Hospital Complaints Procedure will be followed where complaints need to be raised or addressed.

6. ACCESS TO INFORMATION

All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 1998. While there is no requirement to consult with third parties under FOIA, the parties to this agreement will consult the party from whom the data originated and will consider their views to inform the decision-making process. All decisions to disclose must be recorded by the disclosing organisation.

Each Partner Organisation shall publish this agreement on its website and refer to it within its Publication Scheme. If a Partner Organisation wishes to withhold all or part of the agreement from publication it shall inform the other Partner Organisations as soon as reasonably possible. Partner Organisations shall then endeavour to reach a collective decision as to whether information is to be withheld from publication or not. Information

shall only be withheld where, should an application for that information be made under FOIA 2000 it is likely that the information would be exempt from disclosure and the public interest lie in favour of withholding. However, nothing in this paragraph shall prevent the individual Partner Organisations from exercising its obligations and responsibilities under FOIA 2000 as it sees fit.

Article 15 of the General Data Protection Regulation 2016 provides individuals the right to have access to information held about them with limited exemptions. It is necessary to ensure that only appropriate access to information is granted therefore the agreement must detail the responsibilities of each organisation to ensure individuals rights are met appropriately. The Freedom of Information (FOI) Act (2000) gives everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

Each party will deal with any such requests in line with their own policies and procedures.

7. INDEMNITY

Each partner will keep the Data Controller fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner, of any data obtained in connection with this agreement.

8. REVIEW OF DATA SHARING AGREEMENT

This section should define how and when the agreement will be reviewed and audited. It is recommended that each agreement is reviewed one year after signature and at an agreed period thereafter. This review is the responsibility of the Data Controller.

9. CLOSURE/TERMINATION OF AGREEMENT

Any partner organisation can suspend this agreement for 45 days if security has been seriously breached. This should be in writing and be evidenced.

Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the signatories of this agreement, or their nominated representative. This meeting to take place within 14 days of any suspension.

Termination of this Data Sharing Agreement should be in writing to all other Partner Organisations giving at least 30 days' notice.

10. SIGNATORIES

Each partner should identify who is the most appropriate post holder within their agency to sign the agreement having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their organisation to the indemnity. In most cases it will be the organisation's Caldicott Guardian who will be signatory to data sharing agreements. It is the responsibility of the individuals identified at 3.2 to ensure that copies of the agreement are made available as necessary to ensure adherence to the agreement.

Signatories:

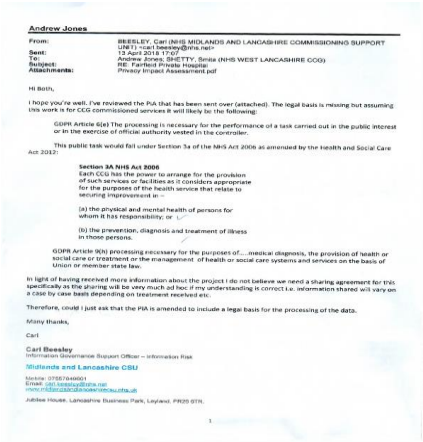
Name		Name	
Role		Role	
Organisation		Organisation	
Signature		Signature	
Date		Date	

Name		Name	
Role		Role	
Organisation		Organisation	
Signature		Signature	

Date		Date	

11. APPENDIX 1 – PRIVACY IMPACT ASSESSMENT

Privacy Impact Assessment for electronic transfers of patient information:



Andrew Jones

From: BEESLEY, Carl (NHS MIDLANDS AND LANCASHIRE COMMISSIONING SUPPORT UNIT) <carl.beesley@nhs.net>
Sent: 13 April 2018 17:07
To: [redacted] (NHS WEST LANCASHIRE CCG)
Subject: RE: Fairfield Private Hospital
Attachments: Privacy Impact Assessment.pdf

Hi Both,

I hope you're well. I've reviewed the PIA that has been sent over (attached). The legal basis is missing but assuming this work is for CCG commissioned services it will likely be the following:

GDPR Article 6(e) The 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.

This public task would fall under Section 3a of the NHS Act 2006 as amended by the Health and Social Care Act 2012:

Section 3A NHS Act 2006
Each CCG has the power to arrange for the provision of such services or facilities as it considers appropriate for the purposes of the health service that relate to securing improvement in –

(a) the physical and mental health of persons for whom it has responsibility, or

(b) the prevention, diagnosis and treatment of illness in those persons.

GDPR Article 9(h) processing necessary for the purposes of.....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.

In light of having received more information about the project I do not believe we need a sharing agreement for this specifically as the sharing will be very much ad hoc if my understanding is correct i.e. information shared will vary on a case by case basis depending on treatment received etc.

Therefore, could I just ask that the PIA is amended to include a legal basis for the processing of the data.

Many thanks,

Carl

Carl Beesley
Information Governance Support Officer – Information Risk
Midlands and Lancashire CSU
Mobile: [redacted]
Email: [redacted]
[redacted]
Jubilee House, Lancashire Business Park, Leyland, PR25 3TR.