Medway NHS
NHS Foundation Trust

Privacy Impact Assessment

Project: **Electronic Order Communications Project (Order Comms)**

Release: 1st Revision of 2nd Formal Issue

Date: 03/06/16

Author: Chris Stiff, IT Programme Manager

Owner: Dr. Maadh Aldouri, Clinical Director for Haematology, Pathology and Cancer

Document Ref: EOC-PIA-001

Version No: v2.1

1 Document History

1.1 Document Location

This document is only valid on the day it was printed. The source of the document will be found at this location:

S:\Health Informatics PMO\Electronic Order Comms Project\Management Products\Privacy Impact Assessment

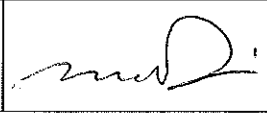
1.2 Revision History

Revision date	Previous revision date	Summary of Changes	Changes marked?
05/06/15	26/05/15	2nd draft	No
08/06/15	05/06/15	1st Formal issue	No
20/05/16	08/06/15	2nd formal issue. Changes reflecting the need to make patient-identifiable data available to external suppliers for Radiology and Pathology data cleansing activities.	No
03/06/16	20/05/16	Changes to document owner and approval	No

1.3 Approvals

This document requires the following approvals.

Signed approval forms should be filed appropriately in the project filing system.

Name	Signature	Title	Date of Issue	Version
Dr. Maadh Aldouri		Clinical Director for Haematology, Pathology and Cancer	08/06/16	

1.4 Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version
Lynne Stuart	Director of Corporate Governance, Risk, Compliance & Legal	03/06/16	v2.1
Dr. Maadh Aldouri	Clinical Director for Haematology, Pathology and Cancer	03/06/16	v2.1

2 Table of Contents

3 Guidance

Summary of Project, Process or Initiative	The project will be completed in phases with the initial phase focusing on enabling acute clinicians and external service users (GPs, Prisons, Army etc) to request pathology and radiology diagnostic tests electronically and receive results in the same way. The implementation will largely negate the need to complete handwritten request forms, of which there are multiple types in use and will significantly improve data quality and reduce the overall diagnostics timescale.

Why should I do a Privacy Impact Assessment (PIA)?	The principle behind PIA's is to look at the privacy risks associated with a new project or piece of work and to see if you can use less privacy invasive options.
When should I complete a PIA?	A PIA should be undertaken at the start of a project or initiative and certainly before equipment or services are purchased.
Who should complete a PIA?	**Stage 1** below should be completed by project managers, leads for new initiatives and service commissioners / procurement managers. **Stage 2** below should then be completed with the Information Governance Team.
Who signs off PIAs?	The Information Governance Steering Group will review the completed PIA.
Data Flow Mapping	The data flows identified in this PIA must be added to your departmental Data Flow Map. Contact your manager or the IG team to see your current map.
How should I record residual risk?	**Any residual risks identified after conducting this PIA must be added to your Corporate Risk Register. This PIA cannot be signed off until this has been completed.**

4 Definitions

Person Data	All data about patients, public or staff is referred to as personal data This includes data that can **identify** a person as well as information **about** that person e.g. health or staff records.
Anonymous record	All data that can potentially identify an individual, whether alone or in combination with other data, has been deleted.
Pseudonymised record	PID is replaced with a pseudonymised identifier. E.g. AB4878 replaces name. This must allow the new identifier to track back to the original record. Other examples. Address becomes Tonbridge, or Kent. Date of birth (26/12/74) becomes age 36.

5 Stage 1: Data Processing

				To be completed for YES answers ONLY		
	Question	Guidance	Y/N	What changes are there?	What are the privacy risks?	How will you mitigate the risks?
1.	Is new or additional technology being used that has substantial potential for privacy intrusion?	E.g. biometrics, surveillance, digital image recording, new statistical analysis & logging of electronic traffic.	N			
2.	Are new identifiers being introduced? Are existing identifiers being used for a new purpose? Could the purpose be construed as intrusive?	E.g. violent patient crime number E.g. postcode use for patient survey E.g. facial recognition software	N			
3.	Might the status of anonymity or pseudonymity be changed or denied?	Will someone be identifiable where they could not be before?	Y	Patient-identifiable data will need to be made available to external suppliers in order to assist with the database cleansing work for Pathology and Radiology.	Patient-identifiable data will be made available electronically to external suppliers.	1) Ensure information is passed to suppliers via secure servers. E.g. SFTP or local servers that suppliers have remote access to. 2) Ensure that a confidentiality agreement with suppliers is in place that includes the information Governance responsibilities of each party.

				To be completed for YES answers ONLY		
	Question	Guidance	Y/N	What changes are there?	What are the privacy risks?	How will you mitigate the risks?
4.	Are multiple organisations involved?	Data Controller / Processor relationship must be explicit in contract and purpose for information sharing must be clearly documented	Y	once fully implemented, no new / additional organisations are involved. Changes relate only to requests being placed electronically instead of by paper. During the implementation it will be necessary to engage with system suppliers to assist with data cleansing activities.	Under normal operating circumstances – post implementation, privacy risks will lower than currently as data is transmitted electronically and directly between requester and provider service. Currently patients are normally handed paper requesting forms to be taken to e.g. radiology or phlebotomy, which have the potential to be seen by other people who do not have a legitimate need to access the information. During the implementation patient data will be available to system suppliers.	1) Implementing an electronic order comms will reduce existing risks under normal operating circumstances. 2) Ensure that a confidentiality agreement with suppliers is in place that includes the information Governance responsibilities of each party.

				To be completed for YES answers ONLY		
	Question	Guidance	Y/N	What changes are there?	What are the privacy risks?	How will you mitigate the risks?
5.	Is there a new or significantly changed processing of PID or sensitive data?	E.g. use of external network storage	Y	Once fully implemented there will be no significant change in processing of PID or sensitive data. During the implementation it will be necessary to engage with system suppliers to assist with data cleansing activities.	During the implementation patient data will be available to system suppliers.	Ensure that a confidentiality agreement with suppliers is in place that includes the information Governance responsibilities of each party.
6.	Will the processing result in a significant amount of new data being held?	Clear communications are needed to inform patient/staff	N			
7.	Will the processing result in the handling of new data about a significant number of people or a change in the population coverage?	Clear communications are needed to inform patient/staff	N			

				To be completed for YES answers ONLY		
	Question	Guidance	Y/N	What changes are there?	What are the privacy risks?	How will you mitigate the risks?
8.	Will there be new or changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	Issues may arise in relation to data quality and accuracy. New data quality checks may need to be introduced	Y	The introduction of an order comms system will require it to be interfaced to the Trust's Laboratory and Radiology information systems and most likely to Oasis PAS also	Privacy risks are minimal. Systems will be configured to ensure only users with legitimate needs will be able to access data. System access will be auditable at user level.	Through system configuration. Interfacing systems will enable data quality to be improved via patient demographic validation services (spine).
9.	Does the processing involve new or changed data access, sharing, security or disclosure arrangements?		Y	During the implementation it will be necessary to engage with system suppliers to assist with data cleansing activities.	During the implementation patient data will be available to system suppliers.	Ensure that a confidentiality agreement with suppliers is in place that includes the information Governance responsibilities of each party.
10.	Does the processing involve new or changed data retention arrangements?		N			
11.	Does the processing include public security measures or is exempted under law?	E.g. Crime, terrorism, public order and public health	N			

6 Stage 2: Data Protection

To be completed with the Information Governance Team

Question	Guidance	Your Response
Who is Data Controller and Data Processor?		The Medway NHS Foundation Trust is the Data Controller for any information we produce and hold e.g. diagnostic test results / reports. The referring organisations such as GP surgeries will also be Data Controllers for any information they produce and hold such as patient demographics etc.
Please list the ICO registration number for all organisation who will have access to the data		The ICO Registration number for the Medway NHS Foundation Trust is Z5002033. The referring organisations such as GP surgeries, which are too numerous to list will have separate ICO Registration numbers.
What IG contractual arrangements are in place?		The Trust is bound by the NHS Standard Contract 2015/16 and within it General Condition 15 and 21 outlining Information Governance, Data Protection, SIRO and Caldicott Guardian. Locally agreed contracts also refer to Confidentiality and Data Protection and the Acts of Parliament that support them
What personal data are you processing and for what purpose?	E.g. direct healthcare, employment of staff, audit or analysis.	Personal data including demographics, diagnoses and other clinical information for use in direct healthcare e.g. symptoms / clinical presentation, diagnostic test request and results including sensitive results such as HIV and sexually transmitted infections.
On what grounds are you legally processing personal data?	E.g. Consent (implied or explicit) Legal obligations e.g. public health Vital interests e.g. life or death Legitimate interests of the data holder	Implied consent and vital interests depending on circumstances and context e.g. GP and Emergency Department admission.

Question	Guidance	Your Response
If explicit consent is required, how is it obtained and how will dissent to sharing be managed?		Not required as consent is implied
How do you inform individuals how their data is being used?	E.g. ICO registration & Fair Processing [patient advice] leaflets & posters.	Posters and leaflets in appropriate locations within the Trust and information on the Trust website. GP surgeries etc will have their own communications management approach.
If processing existing personal data for a new purpose, do you need to inform the individuals?		Not applicable
Is the new purpose compatible with the original purpose?	E.g. health records used to track missing persons. The purpose is not compatible.	Not applicable
Can you confirm that anyone who will have access to the personal data is current with their annual mandatory IG training?	Link to IGTT	For Trust-based staff, current IG training is mandatory. There will be no new data recipients that are external to the Trust as a result of the system implementation
Have you checked the dataset is relevant, adequate & not excessive?	Refer to the Data Protection Principles & Caldicott Policy.	Dataset will replicate existing system
Do you check data for accuracy [numerical & free text]?		There are no formal checks for data accuracy within the current approach. Implementing an electronic order comms solution will significantly improve data accuracy.
How long will the data be kept for and who is the information asset owner for the data set?		Pathology and radiology departments are mandated to retain records for varying periods, which are complied with in full and in accordance with e.g. CPA / UKAS / ISO requirements.
Describe your data loss contingency & back up plan.	Records may be paper, field based, mobile or network based, etc	The electronic order comms system will not change the existing arrangements for storage and back-ups. Data are currently stored on resilient servers within the Medway Data Centre or at GE in the case of radiology data.

Question	Guidance	Your Response
Are you transferring data out of the UK? If so where?		No
Direct electronic marketing (text, email, phone, fax) must comply with the (PECR) Privacy & Electronic Communications Regulations 2003.		Not applicable
Statutory Compliance conclusion	(DPA, A2HRA, HRA etc). To be completed by the Information Governance Team	

7 Stage 3: Sign Off

The following signatories consider that the data being collected for the purpose of this work is lawful, appropriate and not excessive and that wherever possible, all reasonable steps are being taken to minimise risk and enhance confidentiality. Any residual risks outlined in this assessment and their possible impact has been added to the company risk register.

Signature	
Print name	Chris Stiff
Role	IT Programme Manager
Date	3 June 2016
Signature	
Print name	Lynne Stuart
Role	Director of Corporate Governance, Risk, Compliance & Legal and Senior Information Risk Owner (SIRO)
Date	7 June 2016