Information Governance Report

Executive Summary

The establishment of appropriate Information Governance (IG) practices was identified as being critical to the aims and objectives on the Connected Health Cities (CHC) Programme. To this end the CHC Hub implemented an IG Workstream. The aim of the IG workstream was to deliver IG expertise to the Hub and to each of the regional CHCs; to support and work with the IG leads in each CHC; and to liaise with the IG leads within each of the host organisations to ensure that local policies and procedures were being adhered to. The CHC appointed the Head of Information Governance, an independent IG and Privacy expert, to lead the IG workstream.

The IG Workstream produced a number of key deliverables to assist CHC regions and the Hub in addressing the range of Information Governance issues that were encountered.

A key deliverable of the workstream was the IG Working Group (IGWG) for IG leads across the CHC Programme. The IGWG agreed that documentation to assist with the procedure of getting the required data would be an early requirement. To this end the Head of Information Governance developed a Data Sharing Guidance Document, Data Sharing Contract and Data Sharing Agreement for use by CHC regions. In addition, the implementation and use of an Information Sharing Gateway was also facilitated.

The Head of Information Governance also developed a series of safeguards and controls to be adhered to by each CHC project. The implementation of these, which was monitored by the IGWG, ensured that good IG practice was embedded within each regional CHC.

These safeguards and controls were presented to the two Citizen's Juries to ensure that they provided confidence in the approach being adopted to protect patient privacy. Discussions at these meetings helped to identify more stringent controls that would be required when the CHC data were to be put to broader research uses.

Through the IGWG the Head of Information Governance also assisted CHC regions to develop Privacy Impact Assessments for each project and to prepare for the new Data Protection Legislation (DPA2018 incorporating the EU General Data Protection Regulation).

With colleagues from other workstreams the Head of Information Governance assisted in:

- The Development of a Glossary of Terms which has been published on the CHC website to assist members of the public in understanding the CHC approach;
- An application to record Patient Consent
- Development of an Overarching Privacy Statement for the CHC website

Finally, in collaboration with a regional IG lead, the Head of Information Governance created and ran a workforce development IG workshop to guide attendees on how to address the Information Governance issues involved in establishing data sharing for research projects.

.

Introduction

The CHC Programme aimed to process existing information from primary, secondary and social care to improve health and social care. Although the four CHCs planned to use different systems infrastructure and resources, and to pursue different priorities they all required the expertise and technology to obtain, link and analyse the data allowing patients to be tracked through different services. The aim was to use these analyses to shape health and social care services to deliver better outcomes for patients and communities.

At a very early stage CHC Hub determined that it would be critical to the success of the programme to implement appropriate information governance arrangements to ensure that patient and service user data was shared and processed lawfully and ethically.

As a result a subject matter specialist was appointed as CHC Hub Head of Information Governance to lead an IG workstream which would deliver expertise to the Hub and to each of the regional CHCs; to support and work with the IG leads in each CHC; and to liaise with the IG leads within each of the host organisations to ensure that local policies and procedures were being adhered to.

Approach and Key Deliverables

Information Governance Working Group

An IG Working group (IGWG) was established to provide assurance to both those organisations that were to share data with CHC and to the patients and public. The IGWG's main objective was to ensure that the data would be held securely and used ethically by entrenching good IG practice within each CHC. Representatives from each of the CHCs, in particular those responsible for IG within their area, joined the IGWG. The IGWG met on a monthly basis in the first instance: meetings were moved to every two months towards the end of the Programme when good practices had been embedded into each CHC and therefore there was less business to discuss.

It was recognised that each regional CHC was hosted by an organisation that was the legal entity responsible for the IG practices of the CHC, so it was important for each CHC to ensure that they also complied with local policies and procedures.

Support for Data Sharing Arrangements

A key obstacle to programmes like CHC is the understanding of IG requirements as this can cause data sharing to stall. Another early delivery for the programme was the delivery of supporting documentation for data sharing. This included:

- **Data Sharing Guidance** – a comprehensive guide to the issues to be addressed when seeking data from other organisations including identifying the minimum data required to meet the objectives of a study; how to assess the lawful basis for the processing; the approvals that would be required and the potential documentation required including Data Sharing Agreements and Data Processing Contracts . Preparing to address these issues early in the project is crucial in minimising delays to getting access to the data required.
- **Data Sharing Agreements** – A data sharing agreement was developed for use by CHC with data providers where local arrangements were not already available. A two-stage process was adopted with an overarching **Data Sharing Contract** setting out the key terms and

conditions for any data sharing arrangements and a **Data Sharing Agreement** which describes a specific data flow; the data to be shared; the lawful basis and the purpose the data can be used for.

Registration on the Information Sharing Gateway (ISG)

The ISG is a system designed to assist organisations to develop sharing agreements, identifying and managing risks; managing agreement sign off, and storing the agreements themselves online. The IGWG reviewed the way in which the ISG delivered these objectives and agreed to adopt the ISG as the system to manage their data sharing arrangements. The ISG is now in use in all four CHC regions.

Assistance in applications for Section 251 and Research Ethics Committee approvals

Although most of the CHC programmes were able to deliver their objectives without processing confidential patient information, some were not. For processing to be lawful they either required patient consent or Section 251 (s251) support.

S 251 refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002 which enables the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be transferred to an applicant without the discloser being in breach of the common law duty of confidentiality. In practice, this means that the data controller can, if they wish, disclose the information to the applicant without being in breach of the common law duty of confidentiality.

The Head of Information Governance assisted the programmes that needed to gain such approvals with making their applications and responding to queries that arose during the approvals process.

IG Controls and Safeguards

The Head of Information Governance established a series of IG controls and safeguards that needed to be implemented in order for each CHC to protect their data, mitigate against the risk of a data breach and provide assurance on how data was to be processed. These controls and safeguards were based on those outlined in the Anonymisation Code of Practice[1] issued by the Information Commissioner's Office (ICO) as required by the Data Protection Act 1998. However, CHC included some additional safeguards which went beyond those required for DPA compliance.

The IG safeguards are attached as Appendix A. Progress on the implementation of these safeguards was reported by CHC IG leads to the IGWG.

Citizens Juries

CHC held two Citizens Juries in 2016 to explore whether the planned and potential uses of health data were acceptable to the public. Members of the public, selected to broadly represent the demographic mix of the North of England, were given evidence from, and asked questions of, a range of experts including the Head of Information Governance. These events provided an opportunity to describe the safeguards proposed for protecting the data to be used by the CHC and to gain an understanding from the jurors about their concerns in relation to protecting their data privacy. Most jurors (34 of the 35) found the safeguards were certainly or probably

[1] https://ico.org.uk/media/1061/anonymisation-code.pdf

sufficient for the planned uses of data. However, the jurors were split on whether the safeguards were sufficient when considering potential commercial uses: only 14 of the 36 thought the safeguards were certainly or probably sufficient.

The discussions with the Citizens Juries provided confidence in the proposed approach for the planned uses of data. The findings also enabled the Head of Information Governance to outline more stringent controls that would be required when advising on the Code of Practice for the conduct of research using data held in CHC Trusted Research Environments.

Focus Groups

CHC in the North East and North Cumbria conducted 23 focus groups across the region from May to December 2017 on the sharing of personal medical records. Citizens expressed their hopes, concerns and expectations of the Great North Care Record (GNCR), a new way of sharing medical information by health and social care practitioners as they provide direct patient care. The GNCR allows key information such as diagnoses, medications, details of hospitals admissions and treatments to be shared between the different services. A total of 314 individuals participated in the focus groups, expressing clear values that must underscore any sharing of data held about them. Fundamental to these values was an expectation of respect as evidenced through reciprocity, fairness, agency in decision making, privacy, and transparency/trust. Numerous recommendations were put forward based on the findings, including that citizens be able to update their data sharing preferences as and when it suits them, that no companies or individuals make a profit from public health and social care data, and that governance of the GNCR incorporate both experts and citizens. The results led to further engagement by CHC NENC with minoritized and marginalised social groups in the region to identify more specific concerns among these populations.

Privacy Impact Assessments

In the main, CHCs processed pseudonymised data, although some individual projects required access to confidential personal information. Under the previous Data Protection legislation, a Privacy Impact Assessment would not have been required for projects involving Pseudonymised data. However, in anticipationof the rules changing under the new Data Protection Act in 2018, the Head of Information Governance worked with CHC to develop a Privacy Impact Assessment for each of the projects. The Privacy Impact Assessment identified the risks of the project to patient privacy and how these risks should be mitigated either through the generic safeguards and controls or by the implementation of project specific controls.

The Head of Information Governance and the IGWG facilitated review and discussion of PIA's between regional peers – this provided support for those who were less familiar with the process.

Glossary of Terms

Public Engagement has been a key strand throughout the CHC programme. Collaboration with the CHC Public Engagement Director enabled a Glossary of Terms to be developed which was designed to explain the technical language surrounding the use of patient data in user friendly, plain English. The definitions and explanations used were derived from a number of sources, including Understanding Patient Data and Review of Data Security, Consent and Opt-Outs by The National Data Guardian for Health and Care. The Glossary of Terms is live on the CHC website so that it can be used by the general public.

Privacy / Transparency statements

A privacy or transparency statement is required to explain to patients how their data is obtained, used, disclosed, and managed by each controller. It fulfils the legal requirement for transparency. It is the responsibility of local host organisations to ensure that CHC projects are included within their Privacy Statement, however, a generic Privacy statement was developed for use on the CHC website to explain how each CHC would protect a customer or client's privacy.

Consent models

For those projects that were relying on patient consent as a lawful basis for the common law duty of confidentiality, advice was provided to ensure that consent statements were sufficient to allow the required processing and that patient information sheets supporting the consent models were comprehensive and understandable.

Consent Recording

The CHC technical work stream commissioned a system to enable the recording and management of patient consent in order to legally use and link their health data based on consent. The system will initially be used by the researchers from the Born in Bradford programme to manage data relating to a cohort of mothers and babies. The tool will also be available as freeware to others who are setting up a similar programme. The Head of Information Governance worked with the developers to ensure that the IG implications of the application were embedded within the system being developed.

Introduction to GDPR

Part way through the CHC Programme the data privacy laws were overhauled by the implementation of the Data Protection Act 2018 (DPA2018) which incorporated the new EU data protection regulation referred to as the EU General Data Protection Regulation (GDPR). The IGWG discussed the implications of the GDPR on their projects to identify the actions required to ensure they remained compliant with data protection legislation. In particular, this affected those projects that were using pseudonymised data. Prior to DPA2018 pseudonymised data were considered to fall outside the DPA where appropriate controls were in place. After DPA2018 was introduced this changed and projects were required to ensure that they had a lawful basis for processing the data under the DPA. Each CHC was alerted to the fact that they needed to work with their host IG leads to ensure that the lawful basis they had identified was accepted and included within the host organisations GDPR

Training.

The Head of Information Governance and a regional IG lead created and ran a workforce development IG workshop which were open to anyone involved in health data research. The aim of the workshop was to guide attendees on how to address the Information Governance issues involved in establishing data sharing for research projects. Four case studies from the CHC Programme were used to give the attendees an opportunity to discuss real-life problems and a Question & Answer session at the end of the day allowed them you to raise any issues they had encountered which were not covered in the workshop itself. The demand for the event was so high that a second workshop was held, both were well attended and received excellent reviews. In total 47 people attended the workshop from CHC affiliated organisations from across the North of England; all surveyed attendees rated the session as either ‘good’ or ‘excellent’.

Results - All outputs, even things that did not work, are valuable and should be captured.

The involvement of a Head of Information Governance in the CHC was generally successful. Those involved within each CHC will testify that early assessment of IG issues for each of their projects with an independent expert was of great benefit in reducing delays often attributed to IG issues. The IG Working Group enabled discussion of issues with peers in other projects, although one CHC was less engaged in the group that the others.

The development of safeguards for protecting data and monitoring their implementation resulted in each CHC broadly working to the same standards that had been tested with members of the public as being sufficient to protect their privacy for the uses that the CHC were putting the data to.

The development of Data Sharing documentation was ensured that all necessary clauses for data sharing were adopted. The CHC Data sharing Contract and Agreement documents themselves were of limited use, as not surprisingly, many organisations who were sharing data with the CHC had their own documentation. However, they were used in some projects and they also provided a useful benchmark for CHCs to compare with the documents they were being asked to sign.

The Data Sharing Guidance was useful to forewarn projects of the IG issues they would need to address in order for the data to be obtained from their data sources and assisted the CHC staff in conversations with their local IG leads.

The discussions regarding the impact of GDPR enabled projects to establish a lawful basis and understand the documentation they needed to complete in order to remain GDPR compliant, in particular understanding the difference between patient consent to meet the Common Law Duty of Confidentiality versus GDPR.

Finally, the training sessions were well received and as stated above a second workshop was held to meet the exceptional level of demand with good feedback received from attendees.

Conclusion/Discussion

The IG workstream should be considered as a success. The involvement of an IG expert within programmes of this type is of immeasurable benefit. There is often a lack of understanding of IG issues both within the local projects and sometimes within the host organisations. Through the implementation of an IG workstream the CHC ensured that each project had access to help and advice in tackling their specific IG issues and also embedded consistent good practice in relation to the sharing, holding and processing of data.

Future plans/sustainability

The Data Sharing Guidance will be updated and expanded to provide a CHC IG handbook that can help those involved in similar enterprises to ensure that they successfully address IG issues from the start, rather than mid-way through a project.

The material used in the training sessions have been published and is available on-line for review or for those that might wish to offer a similar session.

Author/Main Contact

Clare Sanderson – Clare.Sanderson@igs-l.co.uk

Appendix A – Safeguards for Protecting Data

S'guard No	Safeguard Description
0	Each programme completes a separate Privacy Impact Assessment
1	The CHC and data contributors apply technical and physical controls on the transfer of data between data sources and the datawells to minimise the risk of unlawful access, data loss and hacking.
2	Data is stored in a secure data centre (see definitions)
3	Controls are implemented to ensure secure data access (see definitions)
4	Contracts with all (inc commercial) Data Processors make clear their responsibilities under the DPA to protect data.
5	All CHC data users are required to sign a confidentiality agreement
6	Data contributors restrict data provided for patients that have registered an objection in line with the recommendations from Dame Fiona Caldicott's report
7	CHCs achieve at least Level 2 (satisfactory) IGT score
8	A communications campaign is implemented in each CHC to ensure that the public are aware of programme.
9	Patient information materials are made available which include details of where to find out more about the programme inc. data sharing and how to object if they do not wish their data to be shared
10	Publish, implement and monitor data sharing rules and processes
11	Publish all approved data sharing and data access decisions
12	Undertake Citizens Juries to ensure public views are understood
13	All requests for data (OR data that could potentially re-identify an individual) are assessed by a CHC Independent Advisory Group by a CHC Independent Advisory Group
14	CHCs include feedback opportunity for the public on their website and this is referred to in public leaflets etc.
15	Each programme should provide feedback on the benefits that have been achieved on the website
16	Where data is shared with other organisations they are required to sign a data sharing contract and agreement for a controlled environment (see definitions)
17	Undertake data quality checks in the construction and maintenance of the datawell
18	CHCs make clear that they will report to the ICO anyone (both internal staff and external organisations) that deliberately attempt to re-identify individuals.
19	CHC implement an IG Framework which includes disciplinary sanctions for those that fail to adhere to the policies and procedures.
20	CHCs implement an incident management process which incorporates lessons learned to be shared across all CHCs
21	Implement validation checks on number of records expected versus number received
22	All decisions in relation to data sharing or publication follow the ICO Code of Practice and IG Alliance Anonymisation Guidance (to be published soon)
23	Requests for data are risk assessed to ensure they are non-identifying
24	Introduce data laboratories instead of sharing data
25	Organisations requesting data are vetted to check that they are capable of receiving and managing the data appropriately

Definition	Characteristics
Secure Data centre	Satisfactory IG Toolkit Level 2 and / or ISO27001 certified
	Stored data is encrypted
	Appropriate cyber security measures are applied to prevent external attack and intrusion
	Copying / extracting data restricted Data Administrator roles
	All data accesses to the datawell are logged traceable to an individual's account. The audit trail is regularly monitored.
Secure Data Access	Internal and external access requires authentication (password and/ or smart card?)
	RBAC restricts data rows and data items that can be accessed
	There is appropriate governance of RBAC approval
Data Sharing Contract & Agreement for a controlled environment	Includes conditions on:
	Restrictions on the use of the data being made available and the purposes for which it may be used
	Requirements on personnel having access to the data including training and background checks
	Organisational and technical arrangements for protecting the data, and controlling access to the data
	Limits on the copying of data or number of copies of data
	Controls over linkage with other data sets and prohibition of attempts to re-identify individuals
	Reporting any data breaches (including accidental re-identification of patient)
	Conditions on data re-use (onward sharing) and publishing
	Data destruction or return when project ends or contract ends, whichever is soonest
	Sanctions for failure to comply with the contract