Paediatric Cryoablation Procedure and Outcomes Registry UK

Study ID: 18BB37

Appendix 1 Security data protocol

Date of most recent review: 5th October 2018

Obsidian Health Ltd

Template Registry - Data security protocol

Outcome of the system

The purposes of the system is to <<>>

The audit is intending to take place from <<>> for a period of <<>> months. Governance

Technical overview

IT Architecture

Application

The system will collect data only from approved and registered users who have a legitimate reason to enter the data. The registered users will enter data via a web form on a browser that will apply validation to the data to ensure data quality. The system will support browsers Microsoft Internet Explorer 8 or above, Chrome & Firefox recent versions.

Database

The database will be hosted in an IL3 compliant and resilient data-centre with daily backups. The database is encrypted at rest.

Name of system	<<>>
Data controller	<<>>

Obsidian Health Ltd

Data transfer

All data will be transferred via HTTPS

Method for de-identification

An irreversible system generated digest (one which does not allow the digest to be reversed to permit the identity of the individual to be determined) will be used to de-identify the data.

The user of the system will be required to use a non-publicly available patient identifier in order to pseudonymise the patient and rendering the system anonymous at the database level

This will allow the internal linkage of records for the same patient at the same time as effectively anonymising the records and not enabling linkage between organisations for the same patient.

The anonymising identifier is not visible to the system user, has no semantic meaning and is uniquely generated before the values are persisted on the database. No data is cached on the browser or application.

The following table shows the identifiable data items that will be anonymised by the system.

Data item	De-identification method	Value stored
Patient Identifier	SHA-2 (256) with appended SALT	digest
Date of birth	Conversion to age by rounding to the first day of month	Month & Year

The data set proposal is in Appendix 1.

Access

Access to the system will be via named and registered users with a legitimate reason for using the system. Access to the system will be removed on termination of the registry

Audit trail

All logins and database changes are logged.

Obsidian Health Ltd

Administration

There are two user administrators who can provide access to the system for registered users. These are:

- ● Glenn Forbes - Obsidian Health Limited
- ● David Jurczyszyn - Obsidian Health Limited

User access

The user can only access the system when they have been registered and has logged on with a

valid password that meets the following password criteria. Users are authenticated individually.

- ● Minimum 8 characters and maximum of 15
- ● Must contain at least one numeric character
- ● Must contain at least one special character
- ● Must contain one CAPITAL or UPPERCASE character
- ● Must contain lower-case characters

The user must agree to the following password standards:

Do Not

- reveal a password to ANYONE
- reveal a password in an email or other electronic communication
- reveal a password to your line manager
- talk about a password in front of others
- hint at the format of a password (e.g., "my family name, Vehicle registration, Partners

  Name, Date of Birth etc")

- reveal a password on any questionnaires or security forms
- share a password with colleagues
- use the "Remember Password" feature of applications
- write down passwords and/or store them anywhere
- store passwords in a file on ANY computer system (including mobile devices) without

  encryption

  As the registry is only available for a fixed period of time, no enforced password change will be made. Users can reset their password by contacting the Obsidian Health Help desk by email.

Data storage

Obsidian Health Ltd

The data will be stored anonymously in an encrypted at rest document oriented database. The retention period of the data will be agreed with the data controller, as the data is exempt from the data protection act due to it being anonymised, the 5 year retention limit does not apply. After agreement of a destruction date, the data will be confidentially destroyed. No data will be transferred out of the UK, data extraction for analysis will be via encrypted files to the data controller.

Caldicott checklist

Justify the purpose for collecting confidential information

The data is being collected for non-direct care by users with a legitimate reason for doing so and will be effectively anonymised. No sensitive data items in relation to identifying patients are being stored.

Only use confidential information when absolutely necessary

No confidential information will be stored in the database.

Use the minimum confidential information that is required

No confidential information will be stored in the database.

Access only on a strict need to know basis

Only approved registered users with a legitimate reason for entering data can access the system.

Everyone must understand their responsibilities

Users will be required to agree to specified terms and conditions for using the system.

Understand and comply with the law

Both the users and the system must agree to comply with the legislation outlined in Appendix 3.

Obsidian Health Ltd

IG Checklist

Principle	Action
Is the project registered with the appropriate organisation?	The Caldicott Guardian and/or local IG will be required to approve the data collection.
Is patient identifiable information throughout your system? (If yes, you may need patient consent and/or the approval the approval of your Caldicott Guardian/ information governance lead.)	No, all data is effectively anonymised at the database level. Patient Identifiers will need to be created and be used by each organisation.
Will you need to anonymise or pseudonymise your data?	The patient identifier will be a locally held pseudonym, not based on any current identifier which is subsequently hashed at the database level. All other identifiers are anonymised
Are those who have access to the data aware of their IG responsibilities?	Yes, they will be required to sign terms & conditions stating the responsibilities.
Have you considered any ethical issues (third party access)?	There is no third party access to the data
Who has access to the data and at what level (identifiable or anonymised)?	Registered users can see identifiable data. System administrators can only see anonymised data.
How will you securely transfer any data?	All data will be transferred via SSL
Where will you store the data, is this a secure area?	The data will be stored at an IL3 compliant UK based data centre.
What is the level of security on any electronic/paper records of your data?	SHA-2 (256) with appended SALT 128 bit SSL
Is there a password policy to protect any electronic data?	Yes, see above.
Who will be the named guardian/owner of the data?	The nominated data controller
Have you identified the retention period and destruction date for the data?	The retention is for the duration of the audit and the data will be destroyed once the

final extract has taken place with agreement with the data controller.

Glossary

IAO	Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process.
IAA	Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.
SHA-2	Is a set of cryptographic hash functions that takes a block of data and returns a fixed size string such that any change to the data will change the string value
SALT	A SALT is an extra string of characters appended to the data to be pseudonymised.
IL3	Accreditation that requires enhanced security to protect sensitive information and is a common requirement for central Government departments and some agencies. Accreditation is based on HMG security standards – these are based on ISO 27001, but with more stringent requirements.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network layered on top of a Secure Sockets Layer.
CAG	Confidential Advisory Group

Obsidian Health Ltd

Appendix 1 - Proposed data set

Data items may be amended, updated or removed during development, the validation rules for each data item will be proposed and agreed with the customer based on NHS Data Dictionary definitions wherever possible.

Patient Identifier
Date of birth - rounded to first day of month
Gender
Date of death

Obsidian Health Ltd

Appendix 3 - Legislation

All organisations handling personal information have to comply with the acts/laws shown below (this includes the use of personal information for clinical audit purposes). The list is not exhaustive and cannot provide authoritative legal advice, but it aims to raise awareness of the laws applying to data sharing/handling, allowing the user to make provisions for the safety of the data at the start of the project.

<< Update with latest GDPR compliance statement >>

Data Protection Act 1998 — An Act to make provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. All data subjects have a right of access to their health records, therefore all records should be traceable whilst in your care. Obsidian Health Limited are registered under the data protection act, registration reference ZA038318.

Freedom of Information Act 2000 — An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them. You may need to respond to requests for information regarding clinical audit projects. Under the terms of the Freedom of Information Act, anyone is entitled to apply for copies of clinical audit reports. You should therefore ensure that when reporting clinical audit results, there is no stated link between audit conclusions and patients/clients or clinicians.

Human Rights Act 1998 — An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights. The Human Rights Act requires that any invasion of an individual's private life is first subject to a test of necessity and proportionality. It is also underpinned by the Data Protection Act 1998.

Computer Misuse Act 1990 — An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

Criminal Justice and Immigration Act 2008 — The Secretary of State may by order provide for a person who is guilty of an offence under section 55 of the Data Protection Act 1998 (c. 29) (unlawful obtaining etc. of personal data) to be liable.

Section 251 of the NHS Act 2006 — Section 251 of the NHS Act 2006 re-enacted Section 60 of the Health and Social Care Act 2001. The terms Section 60 and Section 251, when used in relation to use of patient information, therefore refer to the same powers. These powers allow the Secretary of State for Health to make regulations to set aside the common law duty of

confidentiality for medical purposes where it is not possible to use anonymised information and where seeking individual consent is not practicable.

Common Law Duty of Confidentiality — The Common Law Duty of Confidentiality is not an act but is a key issue in matters of sharing or using personal and/or sensitive information.