Accredited Safe Haven Arrangements

Update for comment from the HSCIC Board

Author: Clare Sanderson

Date: 25 November 2013

Contents

Purpose of Paper

The HSCIC will be required to share potentially reidenfitiable data with Accredited Safe Havens (ASHs) once they have been defined and established. It is therefore vital that the HSCIC are confident that the controls and assurances established by the Information Subgroup of the Informatics Services Commissioning Group are sufficient for the HSCIC to be confident that they have fulfilled the data controllership duties when sharing data with ASHs.

The board are asked to support that the proposed criteria and approach set out in this paper should be submitted to the IG subgroup for consideration.

Background

The Accredited Safe Havens paper submitted to the HSCIC board in October set out the background to the concept of Accredited Safe Havens as described in the 2013 Caldicott Review report *To Share or not to Share* which makes clear that to protect the individual's confidentiality, anonymised information should be used wherever possible when the information is being used for purposes other than in support of direct care. This was reiterated in the HSCIC's *Guide to Confidentiality* which was published in September.

The Caldicott review recognised that data containing a single identifier (e.g. NHS Number) can be treated as anonymised as long as it is not linked Patient Confidential Information (PCD). The Caldicott report refers to this data as *de-identified for limited access (DID4LA)*. This categorisation permits consideration of data linking whilst retaining an anonymised status when undertaken in a controlled environment such as an ASH.

This de-identified for limited access data, when linked to PCD, becomes identified data and therefore without a clear and legal basis this linkage would be considered a data breach.

The Caldicott report specifies that the linkage of PCD (with a clear and legal basis) and linkage of de-identified but still potentially identifiable information from more than one organisation should be done in specialist, well-governed, independently scrutinised environments known as 'Accredited Safe Havens'.

Being an accredited safe haven does not necessarily mean that the organisation is receiving personal confidential data, but does mean it can receive DID4LA.

An ASH works under contractual and legal controls that enable those sharing data (including the HSCIC) to release data to it without breaching confidentiality and the constraints in the 2012 Health and Social Care Act. The controls provide assurances and prohibit an ASH from undertaking activities that would result in an individual being identified. In the absence of these controls it would not be lawful for the HSCIC or others to disclose DID4LA to an ASH.

Therefore, an ASH must be subject to controls, which prevent activity that might result in the identification of service users, prevent onward disclosure of data without appropriate governance and de-identification and satisfy the usual information governance controls. Within the accredited safe haven, de-identified data for limited disclosure or access must not be linked to personal confidential data unless there is a clear legal basis to do so, and contracts must forbid this as this would constitute a data breach.

While data sharing contracts should be used to impose the necessary controls on an ASH it is recognised that NHS contracts are not enforceable between NHS bodies.

Section 251 regulations could be used to provide an equivalent legal bind that could underpin the contractual terms. However, the existing s251 regulations do not meet this requirement and therefore new regulations would be required. If new regulations are developed for this purpose it seems sensible to apply them to every ASH and not just those where there is no commercial contract. A breach of the ASH requirements would therefore be seen as a breach of the Data Protection Act, not just of the contract, and potentially attract a significant fine. The process of submitting and approving new regulations is between six and twelve months.

The HSCIC should support the development of these additional regulations under section 251 to ensure that appropriate legally binding controls are put in place for all organisations.

The Accreditation Criteria

In order that the HCSIC can share data with an ASH and be confident that the privacy and confidentiality of patients will continue to be appropriately protected there are three aspects to be considered.

Organisational Assurance

The organisation that is seeking ASH accreditation must demonstrate that it is fit and proper to be accredited as a safe haven and can provide the required levels of assurance as set out in the Caldicott Review. These are attached as Appendix 1.

The independent audit process and guidance for auditors will need to be developed in order that appropriate and consistent levels of assurance can be gained.

Infrastructure Assurance

For any organisation wishing to become an ASH that also has access to identifiable data it will be essential that they can demonstrate (through independent audit of their infrastructure arrangements) that the de-identified data for limited access will be held in a logically separate controlled environment. This will be necessary to provide assurance that the de-identified data cannot be linked with PCD.

Once an organisation has demonstrated though independent audit that it has met the required ASH criteria it can be listed on an ASH register.

Public interest

The final aspect to be considered relates to the individual data flows. Those organisations that have already been *registered* as ASHs can apply for data to flow. For each individual linkage scenario, the registered ASH will be required to define the data required, the business purpose for the data, and proposed data linkages to be undertaken. These data flows must be assessed to ensure that potentially reidentifiable data is indeed required; that the business purpose cannot be met through using anonymised data and that the public interest to be gained from the business purpose justifies this.

The assessment of the individual data flows or linkage scenarios could be carried out by a group such as the Confidentiality Advisory Group using a streamlined process.

One a linkage scenario has been approved, then a registered ASH would be accredited for that scenario. The time limited accreditation would then be added to the register.

Recommendations

It is recommended that the proposals as set out, underpinned by a rigorous implementation will provide sufficient assurance for the HSCIC to allow data to be shared with ASHs. Therefore these proposals should be shared with the IG subgroup of the ISCG for their consideration.

Appendix 1- Organisational Assurance

The Caldicott Review identified the need for a consistent national minimum standard of data stewardship, with the leadership (Boards or equivalent body) of organisations with accredited safe havens held accountable for any failings. This was to be supported by a system of external independent audit, which is published, and an accreditation process for all organisations that act as an accredited safe haven. These were:

- Attributing explicit responsibility for authorising and overseeing the anonymisation process e.g. through a Senior Information Risk Officer.
- Appropriate techniques for de-identification of data, the use of 'privacy enhancing technologies' and re-identification risk management.
- The use of 'fair processing notices'.
- A published register of data flowing into or out of the safe haven including a register of all data sets held.
- Robust governance arrangements that include, but are not limited to, policies on ethics, technical competence, publication, limited disclosure/access, regular review process and a business continuity plan including disaster recovery.
- Clear conditions for hosting researchers and other investigators who wish to use the safe haven.
- Clear operational control including human resources procedures for information governance, use of role-based access controls, confidentiality clauses in job descriptions, effective education and training and contracts.
- Achieving a standard for information security commensurate with ISO27001[61] and the Information Governance Toolkit
- Clear policies for the proportionate use of data including competency at undertaking privacy impact assessments and risk and benefit analysis.
- Standards that are auditable.
- A standard template for data sharing agreements and other contracts that conforms to legal and statutory processes.
- Appropriate knowledge management including awareness of any changes in the law and a joined up approach with others working in the same domain.
- Explicit standard timescales for keeping data sets including those that have been linked, which should be able to support both cohort studies and simple 'one-off' requests for linkage.