echogenicity

September 2019

www.echogenicity.co.uk

Privacy Impact Assessment Policy

Scanning Cornwall's Hearts

Table of Contents

Adherence to the policy should be observed by all staff, contractors and partner organisations working on behalf of Echogenicity that introduce new processes or systems that are likely to involve a new use or significantly change the way in which personal data is handled.

The policy supports the organisation's strategic aims and objectives of enabling Echogenicity to be compliant with privacy, data protection and confidentiality. All employees throughout the organisation need to identify when Privacy Impact Assessment screening and Privacy Impact Assessment itself is required. The assessment of risk in relation to privacy requirements is also required. The policy fits within Echogenicity organisational business risk framework; privacy and information risk need not be managed separately.

September 2019, Next Review September 2021

1. Introduction

The policy is based on guidance originally set out by the Information Commissioner in the Privacy Impact Assessment Handbook Version 2, published in July 2009. This gives guidance from the perspective of the Information Commissioner.

Privacy Impact Assessment (PIA) has been mandated in the NHS by David Nicholson, in his letter dated September 2008. It is also a requirement of the Information Governance Toolkit Version 8.

This policy lays the framework for a formal assessment to ensure that new processes that are introduced meet confidentiality and data protection requirements.

2. Definitions

Privacy Impact Assessment (PIA's)– are structured assessments of the potential impact on privacy for new or significantly changed processes. The PIA should form part of the overall risk assessment of the process or project.

3. Equality Impact Assessment

Echogenicity aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

As part of its development, this strategy and its impact on equality have been reviewed in line with the Equality and Diversity Policy. The purpose of the assessment is to minimise and if possible remove any disproportionate impact on employees on the grounds of race sex, disability, age, sexual orientation or religious belief. No detriment was identified.

The Equality Impact Assessment Tool has been used to help consider the needs and assess the impact of this policy and has been completed alongside this document.

4. Good Corporate Citizen

As part of its development, this policy was reviewed in line with the Good Corporate Citizen Action Plan. The implementation of this strategy promotes good governance.

5. Duties

Echogenicity owns the Privacy Impact Assessment Policy and its implementation. The Chief Executive is responsible for developing and implementing this policy and for reviewing it regularly to ensure that it remains appropriate to the business objectives.

The policy should be published and communicated to all employees, relevant external parties including delivery partners, as should the associated Privacy Impact Assessment template and guidance at Appendix 1.

A hard copy of this policy is kept in Echogenicity's head office.

6. Privacy Impact Assessment

Managing privacy effectively and in line with current guidance and best practice is an important means of enabling the effective use of information for the public benefit, and for assuring all concerned that their information is managed safely and securely and used appropriately.

Privacy is wider than data protection and also concerns people's activities.

Managing privacy and information risks supports the business strategy and objectives including where the organisation can only influence its delivery partners.

The organisation's procedural approach to Privacy Impact Assessment is set out in the PIA template and associated guidance at Appendix 1.

PIA's help the organisation to:

- Anticipate and address likely impacts;
- Identify privacy risks to individuals;
- Foresee problems;
- Enable the timely location and retrieval of personal information to meet the requirements of Subject Access requests.
- Negotiate solutions;
- Protect the organisation's reputation.

Echogenicity, has agreed plans to introduce the necessary changes in culture to ensure that privacy is valued, protected and used for the public good.

The requirements for Information Governance Privacy Impact Assessment awareness training are included in an in-house training package, and individual consequences of failure to apply the organisation's policies and practices are regarded as serious disciplinary issues.

Privacy Impact Assessment Screening, and where appropriate, Privacy Impact Assessment, is a part of all new projects, policies and procedures and should be considered at the initiation stage.

All new projects, procedures and policies will require screening for Privacy Impact Assessment at the initial stages and prior to any procurement decisions being made.

All Privacy Impact Assessments will be carried out by the Chief Executive.

All potential providers of services/products will be required to include privacy considerations where appropriate, when responding to tender exercises.

7. Risk Management Strategy Implementation

7.1. Implementation

There are published Information Governance policies associated with the failure to adopt departmental procedures on handling sensitive data and these must be considered alongside the PIA template and associated guidance.

Significant privacy risks will be recorded on the Corporate Risk Register, alongside Corporate Risks.

Conducting a PIA is a requirement set out in the Information Governance Toolkit.

All new staff will be made aware of this policy as part of the workplace induction at all organisational levels.

7.2 Training and Support

No further training identified. Support available from Chief Executive.

7.3 Dissemination

Once ratified this policy will be printed and kept in Echogenicity's Head office. All staff will be made aware of its existence via email.

7.4 Storing the Procedural Document

A hard copy will be kept in Echogenicity's head office.

8. Process for Monitoring Effective Implementation

The intent set out within this policy is applicable across Echogenicity and its delivery partners, and contains sufficient detail to ensure consistency across Echogenicity's full range of business environments and functions.

External accountability and progress reporting are facilitated through agreed external audit and IG Toolkit reporting mechanisms.

Incident reporting, recovery and contingency policy and procedures are published and followed; these include issues relating to privacy.

Privacy Impact Assessment Policy

The policy's effectiveness will be monitored and reviewed periodically through the Echogenicity's Chief Executive.

9. Associated Documentation

This document references the following supporting documents which should be referred to in conjunction with the document being developed.

Information Security Policy

Information Risk Policy

Data Protection Policy

Information Governance Policy

Confidentiality Policy

Records Management Policy

10. References

The Data Protection Act 1998

Human Rights Act 1998

Common Law of Confidentiality

Code of Practice for the Use of Passwords

Code of Practice for Storing and Managing Information on Network and Local Drives

CCTV Code of Practice

BS ISO/IEC 27001:2005 & 27002:2005

Information Commissioner's Handbook on Privacy Impact Assessment.

Privacy Impact Assessment Policy

Appendix 1 Privacy Impact Assessment Report

Project Title: Date:

Project Lead:

Project Description:

(enter summary of project, multiple organisations involved)

Assessment Questions Yes / No

1) Does this project involve information about people? If Yes continue. If No then go to sign off page 7.

2) If this project does involve information about people can the person be identified? For example: NHS number; surname and DOB; surname and postcode; photograph; distinguishing features; etc.

If Yes continue. If No then go to sign off page 7.

Privacy Impact Assessment

This project has had a Privacy Impact Assessment completed

- there are no privacy impacts identified.
- the following privacy impacts have been identified:

(*delete as appropriate)

Privacy Impact Assessment Policy

Assessment Question

Delete as appropriate

Comments

Technology

(1) Does the project apply new or additional information technologies that have substantial potential for privacy intrusion? (examples include but are not limited to smartcards, visual surveillance, digital image and video recording, IT systems)

Yes/No If yes, what?

Considerations include:

- Whether all of the information technologies that are to be applied in the project are already well understood by the public
- Whether their privacy impacts are all well-understood by the organisation, and by the public
- Whether there are established measures that avoid negative privacy impacts, or at least reduce them to the satisfaction of those whose privacy is affected
- Whether all of those measures are being applied in the design of the project Justification

(2) Has the justification for the new data-handling process been made clear or published (for example have the benefits, to people or society by implementation of this project, been communicated)?

Yes/No

- Individuals are generally much more accepting of measures, even those that are somewhat privacy intrusive, if they can see the benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed for 'security reasons' or to 'prevent fraud' are much less likely to calm public disquiet.

Identity

(3) Does the project involve: Yes / No

a) the use of a new identifier

b) re-use of an existing identifier

c) additional use of an existing identifier

d) intrusive identification

e) new or substantially changed identity authentication requirements that may be intrusive or onorous

f) identity management processes (examples of identifiers include NHS number, National Insurance number, payroll number, name and dob, name and postcode, first name and surname)

4) Does the project involve use of a new identifier to be used for more than one purposes?

Yes / No

- The public understands that an identifier enables the organisation to collate data about an individual and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly onorous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.

(5) Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously (such as manual systems converted to electronic systems) into identified transactions?

(an important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity – ie is there an absolute need to know for example for a smoking cessation project)

Yes / No

Multiple Organisations

(6) Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives such Yes/No as with adult social care) or private sector organisations (eg as outsourced service providers or as 'business partners' such as hospices, nursing homes etc)?

- Data silos and identity silos may raise issues with data protection legislation
- Particular care is needed in preparation of business cases justifying privacy intrusive projects involving multiple organisations and compensatory protection measures should be considered

Data

(7) Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals such as personal sensitive data including religious beliefs, ethnic origin, health information, protected identities?

Yes / No

(8) Will the project result in the handling of a significant amount of new data about each person, or significant change in existing dataholdings?

Yes / No

(9) Does the project involve new or significantly changed handling of:

a) a considerable amount of individual personal data in a database currently held(for example a bulk upload of a lot of data about each individual though not necessarily a lot of individuals), or

b) personal data about a large number of individuals (for example a bulk upload of personal demographics for purposes other than the original reason for collating it)?

c) new data about individuals

d) new data about a significant number of people

e) a significant change in population coverage

Yes/No

(10) Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

Yes/No

Privacy Impact Assessment Policy

(this is an especially important factor. Issues arise in data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term)

- Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enahnce profiles of them
- The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities such as the transfer of data , the consolidation of data holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (eg to support so called 'front end verification') and the matching of personal data from multiple sources Data Handling

Office Mobile: 07590 234 865 Administrator: jemma.cassidy@nhs.net Visit: www.echogenicity.co.uk
Echogenicity Limited, 2 Beacon House, Beacon Road, St. Agnes, Cornwall TR5 0NE
Company Registration No: 5690772

(11) Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory?

Yes/No

(12) Does the project involve new or changed data collection policies or practices that may be unclear or intrusive?

Yes/No

(13) Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory?

Yes/No

(14) Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?

Yes/No

(15) Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?

Yes/No

(16) Does the project involve new or changed data retention arrangements that may be unclear or extensive?

Yes/No

Exemptions and Exceptions

(17) Does the project relate or give rise to new or changed data handling which is in any way exempt from legislative privacy protections?

(Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions)

Yes/No

(18) Does the project's justification include significant contributions to public security measures?

Yes/No

- Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight.
- This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme

(19) Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?

Yes/No

- Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically accessible form, or outsourcing of aspects of the data handling to sub contractors.
- Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Data Protection Act or other relevant statutory provisions such as where they are in a foreign jurisdiction. Concern may also arise in the case of organisations within the UK which are subsidiaries of organisations headquartered outside the UK.

Question

No

Issues and Comments from

IG Officer and Data Protection Officers

Solutions Target Date:

Chief Executive:

Signed: .....

Date: .....

Appendix 2 – Data Protection and Caldicott Principles

Data Protection Principles of the Data Protection Act 1998

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures that an adequate level of

protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Further information on Data Protection Subject Access rights can be found in the Access to Health Records Policy.

For matters relating to children, please refer to the Children's Act 1989 and subsequent 2004 amendment.

Caldicott Principles

1. Justify the purpose(s);

2. Don't use patient identifiable information unless it is absolutely necessary;

3. Use the minimum necessary patient-identifiable information;

4. Access to patient identifiable information should be on a strict need-to-know basis;

5. Everyone with access to patient identifiable information should be aware of their responsibilities;

6. Understand and comply with the law.

Equality Impact Assessment Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

Yes √

No X

Comments

1. Does the document/guidance affect one group less or more favourably than another on the basis of:

- Race X
- Ethnic origins (including gypsies and travellers)X
- Nationality X
- Gender X
- Culture X
- Religion or belief X
- Sexual orientation including lesbian, gay, transgender and bisexual people X
- Age X
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems X

2. Is there any evidence that some groups are affected differently? NO

3. If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?

N/A

4. Is the impact of the document/guidance likely to be negative?

N/A

5. If so, can the impact be avoided? N/A

6. What alternative is there to achieving the document/ guidance without the impact?

N/A

7. Can we reduce the impact by taking different action?

N/A

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Chief Executive, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact the Chief Executive.