Health Informatics Centre
University of Dundee

IS 802159

IS 802159

Legal and Governance Policy

PURPOSE

To provide a central document containing information about laws and policies that relate to HIC Services SOPs, including a legislation register and, in more detail:

- The GDPR Data Protection Principles
- The 6 Caldicott Principles
- Differentiating Audit, Service Evaluation & Research

SCOPE

This SOP Appendix provides guidance to HIC SOP users as to the key legal and governance policies for the environment in which HIC is operating.

RESPONSIBILITIES

ROLE	RESPONSIBILITY
HIC Operational Director	Accountable for HIC ISMS.
Information Security & Governance Manager	Responsible for HIC ISMS by leading on the compliance and framework of processes.
HIC Process Manager	Leading and deciding on the review and development of their processes. Providing training on SOPs and WIs relating to their team. Ensuring SOPs and WIs are followed and adhered to by their team.
HIC All Staff	Supporting, coordinating, and driving the initiation, review, implementation, communication, documentation, and training of processes and that which it is governed by - ISMS. Adherence to Policy, SOPs and WIs.
HIC Operational Committee	Review and approve SOPs, Policy, and Key Documents.
HIC Executive Committee	Review and approve SOPs, Policy, and Key Documents.
HIC Information Security and Governance Committee	Oversight of policy and SOPs.

HIC Customers/Clients	Adherence to Policy and SOPs.

LEGISLATION REGISTER

Legislation	**Applicability**
Official Secrets Act 1989	
Data Protection Act 2018, incorporating General Data Protection Regulations (GDPR)	√
Human Rights Act 1998	√
A Charter for Safe Havens in Scotland 2015	√
Freedom of Information (Scotland) Act 2002	√
Environmental Information (Scotland) Regulations 2004	√
Disability Discrimination Act 2005	√
Sex Discrimination Act 1986	√
Computer Misuse Act 1990	√
Telecommunications Act 2003	√
Telecommunications (Fraud) Act 1997	√
Electronic Communications Act 2000	√
Telecommunications (Lawful Business Practices) Act 2000	√
Privacy and Electronic Communications Regulations	√
Regulation of Investigatory Powers Act 2000	√
Anti-Terrorism, Crime & Security Act 2001	
Criminal Justice & Public Order Act 1994	
Crime & Disorder Act 1998	
Police & Criminal Evidence Act 1984	√
Civil Evidence Act 1968	√
Data Retention & Investigatory Powers Act 2014	
Civil Contingencies Act 2004	√
Copyright Act 1956	√
Copyright, Design & Patents Act 1988	√
Copyright (Computer Programs) Act 1992	√
Companies Act 2006	√

Police Act 1997	√
Rehabilitation of Offenders Act Scotland 1974	√
Consumer Protection (Distance Selling) Act 2000	
Immigration, Asylum & Nationality Act 2006	√
Fire (Scotland) Act 2005	√

POLICY

GDPR Data Principles

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

"(a) Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Caldicott Principles

(The Caldicott Committee (December 1997), Dept of Health)

HIC Services procedures are also designed to comply with the 6 NHS Caldicott Principles. HIC Services minimises the use of identifiable data - any request for use of identifiable data is referred for specific Caldicott Guardian approval. HIC Services provides a safe environment to implement Caldicott-approved use of data.

1. **Justify the purpose(s):** Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
2. **Don't use patient-identifiable information unless it is absolutely necessary:** Patient-identifiable data items should not be used unless there is no alternative.
3. **Use the minimum necessary patient-identifiable information**: Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.
4. **Access to patient-identifiable information should be on a strict need to know basis:** Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.
5. **Everyone should be aware of their responsibilities:** Action should be taken to ensure that those handling patient-identifiable information, (both clinical and non-clinical staff) are made fully aware of their responsibilities and obligations to respect patient

confidentiality.

6. **Understand and comply with the law**: Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

The Information Governance Review, April 2013 (known as Caldicott 2), added a 7th Principle:

7. **The duty to share information can be as important as the duty to protect patient confidentiality:** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Differentiating Audit, Service Evaluation & Research

The Health Research Authority (HRA) in its publication 'Defining Research – guidance from NRES' provides a guideline as to whether a project is research, which normally requires NHS REC review, or another activity such as audit or service evaluation, which does not. Projects which do require NHS REC review will normally also require NHS R&D permission(s). This standard also applies to an Approved Project requiring data from HIC Services.

From 'Defining Research'. The Health Research Authority (HRA). Ref. 0987 December 2009 (rev. April 2013)

Differentiating clinical audit, service evaluation, research and usual practice/surveillance work in public health

Research	**Service Evaluation***	**Clinical Audit**	**Surveillance**	**Usual Practice** *(in Public Health)*
The attempt to derive generalizable new knowledge including studies that aim to generate hypotheses as well as studies that aim to test them.	Designed and conducted solely to define or judge current care.	Designed and conducted to produce information to inform delivery of best care.	Designed to manage outbreak and help the public by identifying and understanding risks associated.	Designed to investigate outbreak or incident to help in disease control and prevention.
Quantitative research – designed to test a hypothesis. Qualitative research – identifies/explores themes following established methodology.	Designed to answer: "What standard does this service achieve?"	Designed to answer: "Does this service reach a predetermined standard?"	Designed to answer: "What is the cause of this outbreak?"	Designed to answer: "What is the cause of this outbreak?" and treat.
Addresses clearly defined questions, aims and objectives.	Measures current service without reference to a standard.	Measures against a standard.	Systematic, statistical methods to allow timely public health action.	Systematic, statistical methods may be used.

Quantitative research – may involve evaluating or comparing interventions, particularly new ones. Qualitative research – usually involves studying how interventions and relationships are experienced.	Involves an intervention in use only. The choice of treatment is that of the clinician and patient according to guidance, professional standards and/or patient preference.	Involves an intervention in use only. The choice of treatment is that of the clinician and patient according to guidance, professional standards and/or patient preference.	May involve collecting personal data and samples with the intent to manage the incident.	Any choice of treatment is based on clinical best evidence or professional consensus.
Usually involves collecting data that are additional to those for routine care but may include data collected routinely. May involve treatments, samples or investigations additional to routine care.	Usually involves analysis of existing data but may include administration of interview or questionnaire.	Usually involves analysis of existing data but may include administration of simple interview or questionnaire.	May involve analysis of existing data or administration of interview or questionnaire to those exposed.	May involve administration of interview or questionnaire to those exposed.
Quantitative research – study design may involve allocating patients to intervention groups. Qualitative research – uses a clearly defined sampling framework underpinned by conceptual or theoretical justifications.	No allocation to intervention: the health professional and patient have chosen intervention before service evaluation.	No allocation to intervention: the health professional and patient have chosen intervention before audit.	Does not involve an intervention.	May involve allocation to control group to assess risk and identify source of incident but treatment unaffected.
May involve randomisation.	No randomisation.	No randomisation.	No randomisation.	May involve randomisation but

				not for treatment.
Normally requires REC review.	Does not require REC review.	Does not require REC review.	Does not require REC review.	Does not require REC review.

*Service development and quality improvement may fall into this category. Source: NHS HRA

APPLICABLE REFERENCES

- For Definitions see ISMS Glossary

DOCUMENT CONTROLS

Process Manager	Point of Contract
Jenny Johnston	hicbusiness-support@dundee.ac.uk

Revision Number	Revision Date	Revision Made	Revision By	Revision Category	Approved By	Effective Date
1.0	01/01/24	Moved SOP to Confluence from SharePoint and updated into new template	Bruce Miller and Symone Sheane	Superficial	HIC ISMS team member	10/01/24
1.1	10/04/24	Updated document control table and added in revision category	Bruce Miller and Symone Sheane	Superficial	HIC ISMS team member	10/04/24