Healthcare Improvement Scotland Appropriate Policy Document

Data Protection Act 2018
Schedule 1
Appropriate Policy Document

Introduction

This document has been developed to meet the Data Protection Act (DPA) 2018 requirement for an appropriate policy document which covers Healthcare Improvement Scotland’s (HIS) processing of special category and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation (‘UK GDPR’) and Schedule 1 of the Data Protection Act 2018 (‘DPA 2018’).

Purpose

Its purpose is to explain what special category personal data and criminal offence data is processed by HIS, the various reasons for which we use this data, and how we ensure it is handled in accordance with UK GDPR Article 5.

Definitions and Scope

Special category data (Article 9 of the UK GDPR) is personal data which reveals:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person’s sex life or sexual orientation

Sensitive Processing (defined by section 35 of the DPA 2018) is the processing of:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership
- genetic data, or of biometric data, for the purpose of uniquely identifying an individual
- data concerning health
- data concerning an individual's sex life or sexual orientation
Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. Section 11(2) of the DPA 2018 states that criminal conviction data includes data which relates to the alleged commission of offences and related proceedings and sentencing.

Conditions

HIS is a public body established under section 10 of the National Health Service (Scotland) Act 1978, as amended.

HIS processes special category data under the following DPA 2018, Schedule 1 conditions.

**Part 1(1) Employment, Social Security and Social Protection**

HIS may process data concerning racial or ethnic origin, religious or philosophical beliefs, trade union membership, sexual orientation, health and criminal offence data for the purposes of performing its obligations or rights as an employer, or for ensuring the social protection of individuals.

**Part 1(2) Management of health care systems or services or social care systems or services.**

HIS may process data relating to health as part of its statutory functions to provide quality assurance of healthcare which supports the management of healthcare or social care systems or services.

**Part 2(11) Protecting the public against dishonesty etc**  
**Part 2(12) Regulatory requirements relating to unlawful acts and dishonesty**

HIS may process data concerning health and criminal offences for the purposes of its core regulatory functions as defined under section 10E to section 10Z15 of the National Health Service (Scotland) Act 1978 and The Healthcare Improvement Scotland (Requirements as to Independent Health Care Services) Regulations 2011/182.

This includes investigations into the quality and compliance of working practices across a range of independent healthcare providers which may lead to enforcement action being taken in collaboration with NHSS Counter Fraud.

HIS does not process genetic data, or biometric data. HIS does not process personal data concerning political opinion.

**Compliance with Data Protection Principles**

In accordance with the accountability principle, HIS maintains records of processing activities under Article 30 of the UK GDPR and section 61 of the DPA 2018. We carry out data protection impact assessments where appropriate in accordance with Articles 35 and 36 of the UK GDPR and section 64 of the DPA 2018 to ensure data protection by design and by default.

In accordance with UK GDPR Article 37 and based on its status as a UK public authority, HIS has appointed a permanent DPO.

In addition, we have effective breach notification systems and procedures in place that ensure timely reporting to the ICO (where necessary) and appropriate actions are taken to limit the impact of the breach on the affected data subjects.
HIS follows the data protection principles set out in Article 5 of the UK GDPR, and Part 3, Chapter 2 of the DPA 2018 for special category and law enforcement processing, as follows.

**Lawfulness, Fairness and Transparency**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

HIS will:

- task Information Asset Owners to ensure that personal data is only processed where it is lawful to do so
- ensure a lawful basis for processing personal data is identified against each business function, and set out within our Information Asset Register and Records of Processing Activities
- ensure that data subjects are appropriately informed of all processing activities performed by HIS on their personal data (excluding certain areas of law enforcement processing). This will be achieved through the use of a tiered privacy notice published on our website, and just in time notifications where appropriate.

**Purpose Limitation**

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

HIS will:

- task Information Asset Owners to only collect personal data for specified, explicit and legitimate purposes
- ensure all HIS staff and contractors are subject to contractual obligations of confidentiality
- ensure all HIS staff and contractors receive regular information governance training highlighting the limits on purposes for processing personal data
- ensure all special category data are held in systems with robust roles-based access controls
- inform data subjects of those purposes via the published privacy notice and other notification mechanisms
- not use personal data for purposes that are incompatible with the purposes for which it was collected
- inform the data subject before using personal data for a new purpose that is not compatible with the original purpose

**Data Minimisation**

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

HIS will:

- subject new and significantly changed business processes to a DPIA as appropriate
- task Information Asset Owners to only process the minimum personal data needed for the purpose for which it is collected ensure that the data we collect is adequate and relevant
- ensure the least intrusive personal data processing method is adopted in each instance
- periodically review data held and delete anything no longer required
Accuracy

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

HIS will:
• ensure appropriate processes are in place to check the accuracy of the data we create and collect, and to maintain that accuracy for the duration of the processing
• ensure the sources of the personal data we create and collect are reliable
• ensure the individual’s right to rectification is observed and applied in a timely manner

Storage Limitation

Personal data shall be 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.

HIS will:
• task Information Asset Owners to be aware of the personal data held and why it is needed
• determine and justify retention period for personal data
• ensure personal data is destroyed in accordance with HIS’s business classification scheme and disposal policy
• regularly review and erase or anonymise personal data no longer required
• ensure processes are in place that observe and enforce the data subjects’ right to erasure

Integrity and Confidentiality

Personal data shall be 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.

HIS will:
• ensure that there appropriate organisational and technical measures in place to protect personal data in compliance with the NHSScotland Information Security Policy Framework
• maintain Cyber Essentials security accreditation at all times
• provide annual data protection and information security training to all staff
• employ technical security controls to secure sensitive information within systems
• implement role-based access controls to restrict access to sensitive data