Intra NHS Scotland Information Sharing Accord

For NHS organisations in Scotland delivering National Health Service (Scotland) functions.

2023

Document control	
Version	3.0 (2023)
Title	Intra NHS Scotland Information Sharing Accord
Summary	An official Accord between NHS Scotland organisations regarding data sharing for the provision of the National Health Service.
Date	May 2023
Author	SLWG that included IG experts across various NHS Scotland organisations listed in section 8 of the Accord with oversight from Information Assurance and Risk and CMO (Health and Care Directorates, Scottish Government)
Owner	NHS Scotland Chief Executive (Health and Care, Scottish Government)

Version history		
Date	**Version**	**Status/ Summary of changes**
2011	1.0	Published
June 2020	2.0	Published. Amendments to incorporate pandemic situations, final comments from the working group and feedback from Scottish Government.
June 2023	3.0	Published. Minor updates. No fundamental changes in spirit of the Accord.

Contents

INTRODUCTION

1. The complexity of delivering high quality healthcare services means there is a need to facilitate appropriate access in a seamless manner to patients' information throughout the patient journey.

2. In addition, there is increasing emphasis on multi-agency and cross boundary working and management of care which requires professionals to be able to *lawfully, fairly and securely* share *necessary*, *relevant, adequate and proportionate* information in order to provide the best possible care for patients.

3. This requirement is underpinned by the Digital Health and Care Data Strategy and current regulations, including the European Convention of Human Rights, UK Data Protection and Confidentiality legislation, the Public Bodies (Joint Working) (Scotland) Act 2014, the Patient Rights (Scotland) Act 2011 among others, including Network and Information System regulations (altogether the "Privacy and Resilience Legislation").

4. All NHS organisations in Scotland are required to have Information Governance processes in place in accordance with the Scottish Government Cyber Resilience Framework and Scottish Information Sharing Toolkit. Senior Information Risk Owners, Data Protection Officers and Caldicott Guardians are designated roles, to oversee the processing of NHS patient's personal data.

5. For the purposes of this Accord, NHS Scotland organisations refer to the organisations identified in Section 8 of this Accord.

SCOPE AND PURPOSE

6. This Accord has been developed to facilitate the legitimate, justifiable and proportionate sharing of personal data between NHS Scotland organisations for the purposes of provision of services as referenced in sections 1, 1A and 2A of the National Health Service (Scotland) 1978 Act for health care purposes: *"to promote the improvement of the physical and mental health of the people of Scotland*". This Accord should be used for the following health and care delivery purposes:

    a. when there is a need to share or disclose data for the facilitation of patient care between NHS Scotland organisations for purposes compatible with the National Health Service (Scotland) 1978 Act;
    b. for exchange of data pursuant to the management of the healthcare system in Scotland; and
    c. when there is a need to rapidly and safely share data between NHS Scotland organisations in order to monitor and manage public health emergencies.

7. The Data Protection principles and rights established in Scottish and UK-wide legislation should be considered when determining on what information is to be shared under this Accord.

8. The scope of this Accord relates to the sharing of patient and service user information and the exchange of information within the NHS in Scotland, in particular between:

    a. Organisations constituted by the National Health Service (Scotland) Act 1978

        i. Part 1(1) (Health Boards)
        ii. 1(1A) (Special Health Boards)
        iii. section 10 (Common Services Agency)
        iv. those amended by the Public Services Reform (Scotland) Act 2010 and subsequent regulations
        v. organisations constituted by section 3 of The Public Health Scotland Order 2019.

b. Organisations/persons providing services under the National Health Service (Scotland) Act 1978 section 2CB (Functions of Health Boards outside Scotland)

c. Organisations/persons providing services under the National Health Service (Scotland) Act 1978 sections 17AA (Provision of certain services under NHS Contracts)

d. Organisations/persons providing services under the National Health Service (Scotland) Act 1978 sections 17C (Personal medical or dental services), 17CA (Primary medical service: persons) & 17D (Personal dental services: persons).

e. Any other organisations/persons incorporated to the NHS (Scotland) for the provision of health and care services in virtue of the National Health Service (Scotland) Act 1978 section 1A (Duty of the Scottish Ministers to promote health improvement).

For example, this may include, but not be limited to, the sharing or disclosure of information between organisations listed in Part 1 of the NHS Act 1978 namely Health Boards (including Special Health Boards and Public Health Scotland), GPs, Dentists, Hospitals, Prison Medical Staff, Community Pharmacies, Primary Care Contractors as part of the health and care delivery purposes identified in paragraph 5 of this Accord.

This Accord is UK location agnostic (e.g. police premises, etc.) as long as the data flow is required for an NHS Scotland function, service or task within the scope described in section 6 of this Accord. For the avoidance of doubt, all NHS Scotland data flows should comply with any relevant UK or Scottish legislation, e.g. Data Protection, Common Law Duty of Confidentiality, Access to Health Records etc.

9. Generally, the organisations listed in paragraph 8 have a statutory responsibility to provide or arrange for the provision of a range of healthcare, prevention of ill health, health promotion, health improvement and health protection services under National Health Services (Scotland) Act 1978, Public Services Reform Act Scotland) 2010 and the Public Health Scotland Order 2019. NHS Scotland organisations are given these tasks to promote the improvement of the physical and mental health of the population and assist in operating a comprehensive and integrated national health service in Scotland. Further detail is found in individual organisations' privacy notices.

10. For the purposes of the processing in the scope of this Accord, data processing is typically undertaken under UK GDPR Article 6 (1) (e) legal basis and the corresponding Article 9 (2) (h) for health data as special category, however other legal bases may be available depending on the situation:

- UK GDPR Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official functions and section 8 of the Data Protection Act 2018. It should be noted that this is the basis for the majority of information sharing.

- UK GDPR Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services and section 10(1)(c) and Schedule 1(2) of the Data Protection Act 2018.

- UK GDPR Article 9(2)(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject and section 10(1)(e) and Schedule 1(4) of the Data Protection Act 2018.

Other common legal bases used across the NHS Scotland are as follows:

- UK GDPR Article 6(1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- UK GDPR Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject.
- UK GDPR Article 6(1)(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- UK GDPR Article 9(2)(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- UK GDPR Article 9(2)(i) processing is necessary for reasons of public interest in the area of public health and section 10(1)(d) and Schedule 1(3) of the Data Protection Act 2018.

Whilst UK GDPR articles may mention processing in relation of social care, the scope of this Accord is mainly focused on "Intra – NHS Scotland" data flows, therefore, between NHS Scotland organisations (their subcontractors and bodies acting on behalf of NHS organisations) for purposes of patient care, management of NHS services and public health emergencies as described in section 6 of this Accord.

COMMON LAW DUTY OF CONFIDENTIALITY

11. The common law duty of confidentiality is a legal obligation that comes from case law, rather than an Act of Parliament. It has been built up over many years. It is an established requirement within professional codes of conduct and practice and is contained within staff NHS (Scotland) contracts, all of which may be linked to disciplinary procedures.

12. Organisations within this Accord are committed to follow the "NHS Scotland Duty of Confidentiality: Code of Practice".

AGGREGATED (STATISTICAL) INFORMATION

13. Even in situations where information cannot identify an individual it should be shared appropriately, following the applicable governance policies and procedures, and in compliance with any existing legislation and statistical disclosure control protocols or, where applicable, approved through existing approval routes (e.g. Public Benefit and Privacy Panel).

ANONYMISED AND PSEUDONYMISED INFORMATION

14. Anonymised information falls outside the scope of Privacy and Resilience Legislation. Pseudonymised data is within scope of Privacy and Resilience Legislation and should be treated in the same way as identifiable data as it may still be possible to identify individuals, e.g. with rare diseases, drug treatments or statistical analyses within a small population.

WHAT DOES THIS MEAN FOR NHS SCOTLAND ORGANISATIONS?

15. In general terms, NHS Scotland organisations do not require explicit consent to share information among themselves for the provision of healthcare or the management of services, as defined in section "Scope and Purpose" of this Accord, but implicit consent may still be required in accordance with Common Law Duty of Confidentiality.

16. NHS Scotland organisations are not required to develop information sharing agreements in relation to data sharing under Privacy and Resilience Legislation. However, it is good practice to do so, in line with the Information Commissioner's Office. Since 2017, Scottish Government

under delegation of duties by Scottish Ministers, mandated the use of the Scottish Information Sharing Toolkit for NHS Scotland organisations, wherever NHS health data is shared.

17. Organisations under this Accord should take an appropriate risk based approach as to whether additional agreements are required, and wherever possible a pragmatic approach to Information Sharing Agreements must be followed, maximising the application of this umbrella Accord in conjunction with more specific underpinning Data Protection Impact Assessments as appropriate.

18. The parties to this Accord must comply with their legal obligations to produce and review the relevant Data Protection Impact Assessments, and Data Processing Agreements where necessary. NHS Scotland organisations must ensure information is readily available to patients, explaining patients' data rights and the use of their information through an accessible privacy notice.

RESPONSIBILITIES

19. It is recognised that most patients or service users would reasonably expect that information relating to them will be shared appropriately within NHS Scotland organisations, in line with the NHS functions as noted in the "Scope and Purposes" section of this Accord, and that sharing should be undertaken in line with technical and organisational safeguards as mandated by Privacy and Resilience Legislation.

20. NHS Scotland organisations provide these safeguards through demonstrable compliance with legislation, and the implementation of Government guidance such as the Scottish Information Sharing Toolkit, NHS Code of Practice on Patient Confidentiality, the Scottish Government Records Management Code of Practice for Health and Social Care and the Patient's Charter.

21. Patients' personal data must be shared on a strict 'need to know' basis with only the minimum necessary being shared. However, this must include sufficient information to ensure safe care and treatment – missing or incomplete information could present a significant clinical risk.

22. Should a personal data breach or an information security breach occur, the organisations sharing data under this Accord must work promptly together to review, resolve and learn from the breach in compliance with Privacy and Resilience Legislation.

23. Each employee within NHS Scotland organisations involved in the holding, obtaining, recording, using and disclosure of patient identifiable information has a personal responsibility for ensuring the confidentiality and security of such information. Organisations operating under the auspices of NHS in Scotland are responsible for ensuring that staff are trained in information/cyber security, information governance and data protection to an appropriate and reasonable level. Staff are responsible for ensuring that they comply with the training and organisational policies/procedures.

24. Data sharing/disclosure activities must be undertaken using agreed secure methods, these disclosures must be recorded and the receiving organisation must assume responsibilities in line with requirements identified.

25. Information sharing among NHS Scotland organisations that involve processing outside the UK require a separate underpinning Data Protection Impact Assessment and Data Processing Agreements to complement this Accord for such data sharing activities. NHS Scotland organisations utilising overseas processors for their own purposes or to provide services to other NHS organisations should ensure appropriate transfer assessments, impact assessments and processing agreements are in place, and that they are current and monitored for compliance.

GLOSSARY

Item	Description	Reference
Anonymised (Anonymisation)	Information that has had the personal information rendered in such a manner that the individual is not or is no longer identifiable by the recipient of the data.	UK GDPR Recital 26. Further information on this topic may be obtained through the Information Commissioner's website.
Caldicott Guardian	A Caldicott Guardian is a senior adviser within an NHS organisation in areas where Duty of Confidentially is applicable. In Scotland Caldicott Guardians are appointed by Health Boards and each NHS Scotland organisation is required to have a Caldicott Guardian who assists the organisation to uphold the ethical and proportionate use of confidential patient information.	Digital Healthcare Scotland (digihealthcare.scot)
Common Law	Common law, which is also known as case law or precedent is law that has been developed by judges, courts and similar tribunals.	
Cyber resilience framework	The Scottish public sector action plan on cyber resilience sets a commitment to develop a public sector cyber resilience framework. This framework aims to provide a consistent way for Scottish public sector organisations to: • assess their cyber resilience arrangements • identify areas of strength and weakness • gain reasonable confidence that they are adhering to minimum cyber resilience requirements, and • take informed decisions on how/whether to achieve higher levels of cyber resilience on a risk-based and proportionate basis.	Scottish public sector Cyber Resilience Strategy Action Plan Cyber resilience: framework and self-assessment tool.

Data Protection Act 2018	The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).	Data Protection Act 2018
Data Protection Officers (DPO)	The Data Protection Officer (DPO) ensures, in an independent manner, that an organisation applies the laws protecting individuals' personal data. The designation, position and tasks of a DPO within an organisation are described in Articles 37, 38 and 39 of the UK GDPR,	UK GDPR Section 4 Articles 37, 38 and 39. Data protection officers | ICO
European Convention on Human Rights (ECHR)	The European Convention on Human Rights (ECHR) is an international convention to protect human rights and political freedoms in Europe.	European Convention on Human Rights (coe.int)
Information or Data Sharing Agreement	Is a document that sets out between different organisations the purpose of the data sharing, it covers what is to happen to the data at each stage, sets standards and helps all the parties to be clear about their respective roles.	Data sharing information hub | ICO
National Health Service (Scotland) Act 1978	The main legislation providing the framework for the NHS in Scotland.	National Health Service (Scotland) Act 1978
NHS Scotland Code of Practice on Protecting Patients Confidentiality	The code sets out the standards and practice relating to confidentiality for all staff who work in or are under contract to the NHS in Scotland.	Digital Healthcare Scotland (digihealthcare.scot)
Privacy and Electronic Communication Regulation (2003) (PECR)	The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) implement the EU's ePrivacy Directive (Directive 2002/58/EC) and set out privacy rights relating to electronic communications.	Privacy and Electronic Communication Regulation (2003) (PECR)

Pseudonymised (Pseudonymisation)	Pseudonymisation is where personal data has been manipulated so that personal data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately.	GDPR Article 4(5) ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance
Public Services Reform (Scotland) Act 2010	The overarching aim Public Services Reform (Scotland) Act 2010 is to simplify and improve Scotland's public services.	Public Services Reform (Scotland) Act 2010
Records Management Code of Practice	A guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in Scotland.	The Scottish Governments Records Management Code of Practice Information page The Scottish Government Records Management Code of Practice for Health and Social Care 2020
Scottish Information Sharing Toolkit	The Scottish Information Sharing Toolkit is the standard for Scottish public sector bodies who have a need to share personal and non-personal information.	The Scottish Information Sharing Toolkit The Scottish Information Sharing Toolkit approach and tools.
The Security of Network & Information Systems Regulations (N IS Regulations)	The NIS Regulations set out standards security (both cyber and physical resilience) of network and information systems that are critical for the provision of essential services (transport, energy, water, health, and digital infrastructure services).	Security of Network & Information Systems Regulations (NIS Regulations)
UK General Data Protection Regulation (UK GDPR)	The UK General Data Protection Regulation (UK GDPR) is a regulation in domestic law on data protection and privacy for all individual citizens of the UK.	UK General Data Protection Regulation (UK GDPR)