Intra NHS Scotland Information Sharing Accord

For NHS Scotland organisations involved in the provision of health care or the management of health systems and services for the people of Scotland.

Document control	
Version	2.0
Title	Intra NHS Scotland Information Sharing Accord
Summary	An official Accord between NHS Scotland boards regarding business as usual data sharing for established purposes.
Date	June 2020
Author	NHS Scotland Information Governance Forum (SLWG)
Owner	NHS Scotland Information Governance Forum (SLWG)

Version history			
Date	**Version**	**Status/ Summary of changes**	**Author**
2011	1.0	Published	Scottish Government (eHealth)
September 2019	1.1	Initial working draft	SLWG
October 2019	1.2	Subsequent working draft	SLWG
October 2019	1.3	Subsequent working draft	SLWG
November 2019	1.4	Subsequent working draft	SLWG
December 2019	1.5	Draft shared for comment with IG forum	SLWG
January 2020	1.6	Amendments to content based on comments from IG forum members	SLWG
February 2020	1.7	Amendment by SLWG membership and additional IG forum feedback	SLWG
February 2020	1.8	Amendment by SLWG membership following additional IG forum feedback	SLWG
May 2020	1.9	Amendment to incorporate pandemic situations, final comments from the working group and feedback from Scottish Government	SLWG
June 2020	2.0	Approved by the NHS Scotland IG Leads Forum	SLWG

Contents

INTRODUCTION 2
SCOPE AND PURPOSE 2
COMMON LAW DUTY OF CONFIDENTIALITY 4
AGGREGATED (STATISTICAL) INFORMATION 4
ANONYMISED AND PSEUDONYMISED INFORMATION 4
WHAT DOES THIS MEAN FOR NHS ORGANISATIONS? 4
RESPONSIBILITIES 5
GLOSSARY 6

INTRODUCTION

1. The complexity of delivering healthcare systems 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 *securely* communicate and share *necessary*, *relevant, adequate and proportionate* information in order to provide the best possible care for patients.

3. This requirement is underpinned by the UK data protection legislation and the NHS Scotland regulations, as well as the Public Bodies (Joint Working) (Scotland) Act 2014 and the Caldicott Principles. The most recent in regulations and guidance highlight that the duty to share information can be as important as the duty to protect patient confidentiality. The Patient Rights (Scotland) Act 2011 sets out the health care principles, including a commitment to respect an individual's privacy and confidentiality. The Patient Rights (Scotland) Act 2011 places a duty on NHS Scotland Boards to uphold the health care principles, and to ensure that those with whom they enter into contracts, accords or arrangements uphold these principles when delivering healthcare.

4. NHS patients' confidentiality is protected by common law and each individual employee's professional and contractual duties of confidentiality. Also the European Convention on Human Rights, the General Data Protection Regulation (GDPR), UK Data Protection Act 2018 and the Privacy and Electronic Communication Regulation (2003) set the framework within which the privacy rights in relation to the processing of patient information are safeguarded (Privacy Legislation).

5. All NHS organisations have Information Governance processes in place in accordance with the Scottish Government Information Security Policy Framework and have identified Senior Information Risk Owners, Data Protection Officers and Caldicott Guardians who oversee access to, the use of and the sharing of patient personal data with bodies both within, and outside NHS Scotland.

SCOPE AND PURPOSE

6. This Accord has been developed to facilitate the legitimate, justifiable and proportionate sharing of personal data between NHS Scotland organisations as referenced in section 2A of the National Health Service (Scotland) 1978 Act for health care purposes. This Accord should be used:

    a. when there is a need to share or disclose data for the routine facilitation of patient care between NHS organisations for established purposes;
    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 should be considered when determining on the information to be shared under this Accord.

8. Systematic sharing of data should be agreed formally through the application of the Scottish Information Sharing Toolkit underpinned by Data Protection Impact Assessments and relevant Information Sharing Agreements and Data Processing Agreements where necessary.

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

    a. Organisations constituted by the National Health Service (Scotland) Act 1978 section 2 (Health Boards), 2A (Special Health Boards) and section 10 (Common Services Agency) and those amended by the Public Services Reform (Scotland) Act 2010 and subsequent regulations.

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 17C (Personal medical or dental services), 17CA (Primary medical service: persons) & 17D (Personal dental services: persons).

d. 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 Health Boards (including Special Health Boards), GPs, Dentists, Hospitals, Prison Medical Staff, Primary Care Contractors as part of routine health care delivery.

This Accord is 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.

10. Generally, the organisations listed in paragraph 9 have a statutory responsibility to provide or arrange for the provision of a range of healthcare, health improvement and health protection services under National Health Services (Scotland) Act 1978 and Public Services Reform Act (Scotland) 2010. 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.

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

- 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
- 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 Part 1 of the Data Protection Act 2018
- 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 Part 1 of the Data Protection Act 2018

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

- 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

- GDPR Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject

- GDPR Article 6(1)(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person

- 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

- 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 Part 1 of the Data Protection Act 2018

Whilst 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 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

12. The NHS Scotland Code of Practice on Confidentiality says that 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 contracts, both of which may be linked to disciplinary procedures.

13. There is a duty of confidentiality when one person gives information to another person in circumstances where it is reasonable to expect that the information will be kept confidential. The duty of confidentiality is not an absolute right and should be considered in conjunction with all relevant data protection legislation. It is however, generally accepted that the common law allows disclosure of confidential information if:

    - The information provider has consented

    - It is required by law, or in response to a court order

    - It is justified in the public interest

AGGREGATED (STATISTICAL) INFORMATION

14. Where information cannot identify a service user or patient then it is out with the scope of data protection legislation and should be shared appropriately.

ANONYMISED AND PSEUDONYMISED INFORMATION

15. Anonymised information falls outside the scope of data protection legislation. Pseudonymised data 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 ORGANISATIONS?

16. In general terms, NHS Scotland organisations do not require explicit consent to share information between NHS organisations for the provision of healthcare or the management of services.

17. NHS Scotland organisations are not required to develop information sharing agreements for established purposes involving routine business as usual processes. It is considered best practice to develop agreements for non-routine or voluntary information sharing. NHS organisations should develop a risk assessment and review whether an agreement is required in light of their risk appetite.

18. NHS organisations must comply with data protection and privacy legislation, including the completion and regular review of Data Protection Impact Assessments and ensure information is readily available to patients, explaining patients' data rights and the use of their information through an accessible privacy notice.

RESPONSIBILITIES

19. The majority of patients would reasonably expect that information relating to them will be shared within NHS Scotland in order to provide them with care in line with technical and organisational safeguards as mandated by data protection legislation.

20. Controllers provide these safeguards through demonstrable compliance with privacy, safeguarding and public protection 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 patient safety issue. Should an information security breach occur, the organisations sharing data under this Accord will work together to review, resolve and learn from the breach in compliance with GDPR and other legislative requirements.

22. Each NHS Scotland employee 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. Health boards operating under the auspices of NHS Scotland are responsible for ensuring that staff are trained in information governance and data protection to a reasonable level. Staff are responsible for ensuring that they comply with training and organisational policies/procedures.

23. Routine 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. International transfers of information are not permitted under this Accord.

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.	GDPR Recital 26
Caldicott Guardian	A Caldicott Guardian is a senior adviser within an NHS organisation who is responsible for protecting the confidentiality of patient and service-user information. In Scotland Caldicott Guardians are appointed by Health Boards and each NHS Scotland organisation is required to have a Caldicott Guardian	
Caldicott Principles	The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out, at the time of introduction, six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Later, in April 2013 a seventh principle was added. It is noted that this principles are now fundamentally embedded in data protection legislation.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
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	
Data Protection Act 2018	The Data Protection Act 2018 controls how your 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).	http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
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 organization are described in Articles 37, 38 and 39 of the GDPR	GDPR Article 37, 38 & 39
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.	https://www.echr.coe.int/Documents/Convention_ENG.pdf
General Data Protection Regulation (GDPR)	The UK General Data Protection Regulation (GDPR) is a regulation in domestic law on data protection and privacy for all individual citizens of the UK.	http://www.legislation.gov.uk/uksi/2019/419/made

Information 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.	https://ico.org.uk/for-organisations/
National Health Service (Scotland) Act 1978	The main legislation providing the framework for the NHS in Scotland.	http://www.legislation.gov.uk/ukpga/1978/29/contents
NHS Scotland Information Security Policy Framework	Policy guidance that incorporates legal compliance requirements for the Network and Information Systems (NIS) Regulations 2018 and the information security elements of the General Data Protection Regulation (GDPR).	https://www.healthca.scot/information-security-policy-framework/
NHS Scotland Code of Practice on 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.	https://www.gov.scot/publications/
Patient Rights (Scotland) Act 2011	The Patient Rights (Scotland) Act 2011 aims to improve patients' experiences of using health services and to support people to become more involved in their health and health care, The Act requires **Scottish** Ministers to publish a **Charter of Patient Rights and Responsibilities** which summarises the existing **rights and responsibilities** of **patients** using the NHS in **Scotland** and of people with a personal interest in such **patients**' health care. The original (2011) charter has been recently reviewed (2019).	http://www.legislation.gov.uk/asp/2011/5/contents
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.	http://www.legislation.gov.uk/uksi/2003/2426/contents/made
Pseudonymised (Pseudonymisation)	Is where personal data has been manipulated so that the 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)
Public Services Reform (Scotland) Act 2010	The overarching aim of the Act is to simplify and improve Scotland's public services.	http://www.legislation.gov.uk/asp/2010/8/contents
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.	https://www.informationgovernance.scot.nhs.uk/rmcop2020/

Scottish Information Sharing Toolkit	The Scottish Information Sharing Toolkit is the standard for Scottish public sector bodies who have a need to routinely share personal and non-personal information.	https://www.informationgovernance.scot.nhs.uk/istresources/