

Data Protection Impact Assessment (DPIA)

The National Health Service (General Medical Services and Primary Medical Services Section 17C Agreements) (Scotland) Amendment Regulations 2021

1. Introduction

The purpose of this document is to report on and assess against any potential Data Protection Impacts as a result of the implementation of the National Health Service (General Medical Services and Primary Medical Services Section 17C Agreements) (Scotland) Amendment Regulations 2021. (the “regulations”).

2. Document metadata

3.

- 3.1 Name of Project: The National Health Service (General Medical Services and Primary Medical Services Section 17C Agreements) (Scotland) Amendment Regulations 2021
- 3.2 Author of report: Michael Taylor – Primary Care Directorate – GMS Contract Team.
- 3.3 Date of report: 3 September 2021
- 3.4 Name of Information Asset Owner (IAO) of relevant business unit: Naureen Ahmad, Deputy Director.
- 3.5 Date for review of DPIA: 03/09/2024

Review date	Details of update	Completion date	Approval Date

4. Description of the project

4.1 Description of the work:

General Practice is critical to sustaining high quality universal healthcare and to realising Scotland's ambition to improve our population's health and reduce health inequalities.

The regulations reflect the implementation of the removal of certain vaccination services from GP contracts.

The regulations are intended to improve patient access to GP Services, better contribute to improving population health, including mental health, and help to mitigate health inequalities by removing certain vaccinations from GP contracts and thereby allowing GPs to focus on what they do best, such as the management of the needs of patients with complex comorbidities. This will also enhance the GP role to make the profession a more attractive career choice for new and existing GPs.

Health Boards will require appropriate data from GP practices to identify patients for the different vaccination programmes. The 2018 Contract Regulations provided for a legal framework authorising

GPs, on request of the Health Board, to allow access or be provided with data, (contained in patient records or practice data relating to a GP’s practice) or any other information which is reasonably required in connection with the contract.

The Health Board may only make such a request where:

- if the relevant information could be provided in compliance with relevant legislation (Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) (“legislation”);
- if the request is made in accordance with Directions issued by the Scottish Government; and
- it is for the limited purposes of medical diagnosis of, or provision of health care to, patients; planning (including workforce planning and management of health and social care services); or where information is reasonably required (in connection with the contract).

It is intended that the provision/access to data contained in patient records and other related information will be primarily used for medical diagnosis and health care provision, and to increase the numbers of primary care professionals (including pharmacists, mental health workers, community based allied health professionals and nurses) accessing patient information for the purpose of direct patient care. Accordingly, access to patient data for the purposes of direct care may be made available by way of data sharing agreements to appropriate members of the extended primary care team where it is authorised, safe and necessary to do so. It is intended that patient information may also be made available to other health professionals who are providing care to one of a GP contractor’s registered patients – for example, in a vaccination clinic.

4.2 Personal data to be processed.

Variable	Data Source
Medical information of patients.	GP Contractors

4.3 Describe how this data will be processed:

Patient information for the purposes of direct care will be made available to appropriate members of the extended primary care team and to other health professionals, as detailed in section 3.1 of this DPIA, either by direct access to the GP IT system or through an NHS board system. The exact details of how this is done may vary from area to area according to their local information governance arrangements.

Within Scotland data will be transmitted, stored, processed, disposed of, owned and managed in line with current data protection best practice and as specified in Directions.

Any data collected or extracted will only contain the minimum data items required for the purpose, after which it will be destroyed in accordance with data sharing agreements.

4.4 Explain the legal basis for the sharing with internal or external partners:

The 2018 Contract Regulations, and Directions referred to within the 2018 Contract Regulations and any associated data sharing agreement(s) provide the legal framework for processing (and sharing) data. The detail of how data will be collected and shared in practice is contained within Directions.

[PCA\(M\)\(2019\)15 - Joint Controller and Information Sharing Agreement between NHS Scotland Health Boards and GP Contractors](#) was designed to assist Health Boards and GP contractors to determine in a transparent manner their respective responsibilities for complying with data protection legislation.

5. Stakeholder analysis and consultation

5.1 List all the groups involved in the project, and state their interest.

Group	Interest
Scottish Government	Responsible for negotiating the GMS Contract.
BMA	Responsible for negotiating the GMS Contract.
NHS Boards / Integration Authorities	Responsible for commissioning GP Services and workforce planning.
Patients	Service users requiring better coordinated healthcare services.
NHS National Services Scotland	Operation of national systems, central storage of demographic and other data and payments of GP contractors.

5.2 Method used to consult with these groups when making the DPIA.

A series of meetings have been held between Scottish Government officials and the BMA.

Meetings have been held in each Health Board area to discuss the new contract offer with local GPs, and representatives of the NHS Boards and Integration Authorities.

A series of public engagement meetings were being held across Scotland to discuss the new contract offer and plans to transform Primary Care.

Project management of system development and operations involves appropriate stakeholders.

A series of meetings have been held throughout contract negotiations with a reference group comprising of representatives of stakeholders.

5.3 Method used to communicate the outcomes of the DPIA .

The DPIA was copied to appropriate stakeholder groups as part of the submission of the regulations.

6. Questions to identify privacy issues

6.1 Involvement of multiple organisations

The collection, interpretation and use of data will involve Scottish Government, GP contractors, NHS Boards, NHS National Services Scotland and Health and Social Care Partnerships.

6.2 Anonymity and pseudonymity

Where appropriate any person-identifiable data will be pseudonymised at source (in line with SPIRE information governance where this is used). The purpose of the data will define whether it is possible for pseudonymisation to occur as it would normally be the rule: Health Boards will need to identify patients who needed vaccinated.

6.3 Technology

There are no new or additional information technologies that have substantial potential for privacy intrusion. Where collection of information involves the use of the SPIRE system or increasing the range of health professionals who may access SPIRE, this has separately been the subject of a DPIA.

6.4 Identification methods

Existing unique identifiers will be re-used.

There will be no new or substantially changed identity authentication requirements that may be intrusive or onerous.

6.5 Sensitive/Special Category personal data

Where appropriate, personal data may be shared with Scottish Government, GP contractors, NHS Boards and Health and Social Care Partnerships as set out below.

In relation to patient information for the purposes of direct care, this will be available only to those appropriate professionals providing that care according to data protection arrangements.

This may involve the linkage of personal data with health and social care data in other collections in order to, for example, identify gaps in vaccine take up but does not engender any significant change to existing data links or holdings. If any development resulted in a significant change a separate DPIA would be required.

6.6 Changes to data handling procedures

The regulations make no changes to the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before.

6.7 Statutory exemptions/protection

The regulations do not provide for systematic disclosure of personal data to or access by third parties that are not subject to comparable privacy regulation.

The 2018 Contract Regulations authorised that data/information is to be provided upon request by the Health Board which must be made in compliance with relevant legislation, in accordance with Directions and for the limited purposes set out in the 2018 Contract Regulations. Additional protective obligations are set out in the 2018 contract regulations, which obligate:

The GP

To comply with the Health Board's policies concerning data security, personal data or IT security notified by it;

To maintain a record of all its processing activities carried out in the contract;

To nominate a data protection officer (if a jointly designated data protection officer has not been appointed) in matters relating to personal data;

To ensure that any person under its direction who has access to patient records has undergone adequate data protection training; and

To nominate a person with responsibility for practices/procedures relating to confidentiality of personal data held by it and also data protection generally.

The Health Board

To provide guidance, templates and privacy notices relating to the provider's processing of personal data and the contractor's maintenance of a record;

To notify the provider timeously of its current policies regarding data security, personal data security and IT security processes;

To maintain a record of its processing activities carried out in relation to a provider's patient records;

To appoint a jointly designated data protection officer;

To ensure that any of its employees who have access to the patient record and practice data has undergone adequate training; and

To make available appropriate data protection training to the GP provider and its employees.

6.8 +Justification

The project allows information to be shared amongst healthcare providers for the benefit of patients.

6.9 Other risks

There are no risks to privacy not covered by the above questions.

7. General Data Protection Regulation (GDPR) Principles

The 2018 regulations enable the collection, sharing and use of data held by GP contractors. The sharing and use of data is supported by Data Sharing Agreements between Health Boards and practices. This ensures that all involved will be clear about their roles, rights and responsibilities.

SPIRE has already been the subject of a DPIA. Any other systems or mechanisms established for the collection, sharing and use of data will be privacy impact assessed as appropriate – once the precise detail of their operation becomes known.

Principle	Compliant – Yes/No	Description of how you have complied
.1 Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	The Data Agreement between Health Boards and practices ensures that personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject.
Principle	Compliant – Yes/No	Description of how you have complied
6.2 Principle 2 – purpose limitation	Yes	The Data Agreement between Health Boards and practices ensures that personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Principle	Compliant – Yes/No	Description of how you have complied

6.3 Principle 3 – adequacy, relevance and data minimisation	Yes		The Data Agreement between Health Boards and practices ensures that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Principle	Compliant Yes/No	–	Description of how you have complied
6.4 Principle 4 – accurate, kept up to date, deletion	Yes		The Data Agreement between Health Boards and practices ensures that personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
Principle	Compliant Yes/No	–	Description of how you have complied
6.5 Principle 5 – kept for no longer than necessary, anonymization	Yes		The Data Agreement between Health Boards and practices ensures that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
Principle	Compliant Yes/No	–	Description of how you have complied
6.6 GDPR Articles 12-22 – data subject rights	Yes		The Data Agreement between Health Boards and practices ensures appropriate protections and processes are in place for data subject rights. Privacy notices will likely be used to explain the processing of patient data and their rights in this regard.
Principle	Compliant Yes/No	–	Description of how you have complied
6.7 Principle 6 - security	Yes		The Data Agreement between Health Boards and practices ensures that personal data is 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”)
Principle	Compliant Yes/No	–	Description of how you have complied
6.8 GDPR Article 44 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	Yes		Data will not be transferred to a country or territory outside the European Economic Area.

8. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
Regulations do not provide specific detail around the	1.	The Data Agreement between Health Boards and practices obliges and incentivises that data protection	reduced

collection, sharing and use of data held by GP contractors.		requirements are properly complied with.	
			Eliminate/reduce/accept
			Eliminate/reduce/accept

9. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
Regulations are enabling powers and do not provide specific detail around the collection, sharing and use of data held by GP contractors.	1.	Health Boards should be aware of their Data Agreements with practices.	Naureen Ahmad, General Practice Policy

10. Data Protection Officer (DPO)

The DPO may give additional advice, please indicate how this has been actioned.

Advice from DPO	Action

11. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of implementing these regulations has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	Date each version authorised
Naureen Ahmad, Deputy Director, General Practice Policy	03/09/21