

Privacy Impact Assessment (PIA)

The National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018

And

The National Health Service (Primary Medical Services Contracts) (Scotland) Regulations 2018

1. Introduction

The purpose of this document is to report on and assess against any potential Privacy Impacts as a result of the implementation of the National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018 (“GMS”) and The National Health Service (Primary Medical Services Contracts) (Scotland) Regulations 2018 (“PMS”) here referred to together as “the regulations”.

2. Document metadata

- 2.1 Name of Project: The National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018 and The National Health Service (Primary Medical Services Contracts) (Scotland) Regulations 2018
- 2.2 Author of report: Neil Robertson – Primary Care Division – GMS Contract Team.
- 2.3 Date of report: 19 February 2018.
- 2.4 Name of Information Asset Owner (IAO) of relevant business unit: Richard Foggo, Deputy Director.

3. Description of the project

3.1 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 new contractual terms set out in two model contracts will, respectively, reflect the PMS and GMS Regulations when they come into force.

The regulations have common policy intents. For the purposes of this document, unless expressly stated, the policy intent and impact assessments for the regulations and model contract terms will be addressed as one.

The policy, the regulations and the new 2018 contractual terms are intended to improve patient access to GP Services, better contribute to improving population

health, including mental health, and help to mitigate health inequalities. It will also enhance the GP role to make the profession a more attractive career choice for new and existing GPs. It will reduce the risks of becoming a GP Partner, increase the stability of General Practice funding, provide increased transparency on workforce and activity data, improve practice sustainability and improve practice infrastructure.

The regulations provide 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 1988 (DPA) and General Data Protection Regulation (GDPR) ("legislation");
- if made in accordance with Directions; 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 an urgent care setting.

It is intended that the provision/access to practice data (which includes the business aspects of a GP practice) and may include information or data about employees, sub-contractors, remuneration, finances, workloads and contracts, may be used for planning purposes including negotiating future contracts.

It is also intended that aggregate patient demographic data may be gathered securely for planning and improvement purposes.

The detail of the data requirements will be set out in Directions. The Directions will ensure that data processing will be underpinned by robust information governance policies and procedures to ensure that patient confidentiality, and workforce, expenses and workload data is effectively protected.

The framework of responsibilities of Health Boards and GPs are set out in the regulations and will be augmented by Directions, as required.

3.2 Personal data to be processed.

Variable	Data Source
General Practice Workforce data (by staff type and including hours and pay)	GP Contractors
Income and Expenses (GP finances – the costs of running a practice)	GP Contractors
Activity data (consultations)	GP Contractors
Medical information of patients.	GP Contractors

3.3 Describe how this data will be processed:

1. Practice data regarding the business aspects of running a GP practice, which may include income and expenses, will be collected securely. This data will include information regarding the GP practice employed workforce. This data will be used only to inform future contractual negotiations unless agreed otherwise by the Scottish Government and the Scottish General Practitioners' Committee of the BMA. The precise nature of this data will be agreed between the Scottish Government and the Scottish General Practitioners Committee of the BMA and specified in Directions.

2. Aggregate data relating to patients will be collected directly from the NHS IT systems. This will likely include data on the numbers of consultations in GP practices and specific information on the characteristics and medical diagnoses of patients. In the case of GP IT systems this will be done using SPIRE (Scottish Primary Care Information Resource) software or a functional equivalent. If SPIRE is not used to gather data similar, appropriate safeguards to protect data will be put in place.

Aggregate patient data will be accessed and shared with NHS National Services Scotland and/or Scottish Government in line with protocols to be agreed by Directions and in line with the stringent information governance arrangements of SPIRE (<http://spire.scot/professional/safeguards/information-governance/>).

Any data extract will only contain the minimum data items required for the purpose of that extract and for its duration, after which it will be destroyed.

3. 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 PIA, 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.

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

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

4. Stakeholder analysis and consultation

4.1 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 Family Health Service contractors.

4.2 Method used to consult with these groups when making the PIA.

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 are 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.

4.3 Method used to communicate the outcomes of the PIA .

The PIA was copied to appropriate stakeholder groups as part of the submission of the GMS and PMS regulations.

5. Questions to identify privacy issues

5.1 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.

5.2 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.

5.3 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 this has separately been the subject of a PIA.

5.4 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.

5.5 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.

1. To ensure confidentiality data in relation to the General Practice workforce, as well as income and expenses data will be held and processed by NHS National Services Scotland and only anonymised, non-identifiable data for the purposes of analysis will be provided to Scottish Government, NHS Boards or the Scottish General Practitioners' Committee of the BMA. This will be used during Phase 1 of contract implementation to inform the minimum GP Partner earnings expectation and discussion of Phase 2 of the GP Contract negotiations, as well as to support service development and re-design. In Phase 2 (which is subject to further negotiation) it is likely that this data will be required to authorise payments to GPs and provide supporting information to ensure appropriate individual GP practice resourcing.

2. In relation to data on the numbers of consultations in GP practices and specific information on the characteristics and medical diagnoses of patients – to ensure confidentiality this data will either be extracted as aggregates or pseudonymised before being processed.

3. 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, improve care and treatment pathways, but does not engender any significant change to existing data links or holdings. If any development resulted in a significant change a separate PIA would be required.

5.6 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.

5.7 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 regulations authorise 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 regulations.

Additional protective obligations are set out in the 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.

5.8 Justification

The regulations contribute to public health by allowing information to be gathered to support the sustainability and stability of primary care. In particular through service redesign, workforce planning and security of funding. The project allows information to be shared amongst healthcare providers for the benefit of patients.

5.9 Other risks

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

6. The Data Protection Act (DPA) and General Data Protection Regulation (GDPR) Principles

The regulations enable the collection, sharing and use of data held by GP contractors. The precise mechanisms for the collection, sharing and use of data will be explicitly set out in Directions. Directions will also be supported by Data Sharing Agreements where appropriate. This will ensure that all involved will be clear about their roles, rights and responsibilities.

SPIRE has already been the subject of a PIA. 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
6.1 DPA Principle 1 and GDPR Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	Directions will be issued to ensure 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 DPA Principle 2 and GDPR Principle 2 – purpose limitation	Yes	Directions will be issued to ensure 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 DPA Principle 3 and GDPR Principle 3 – adequacy, relevance and data minimisation	Yes	Directions will be issued to ensure 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 DPA Principle 4 and GDPR Principle 4 – accurate, kept up to date, deletion	Yes	Directions will be issued to ensure 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 DPA Principle 5 and GDPR Principle 5 – kept for no longer than necessary, anonymisation	Yes	Directions will be issued to ensure 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 DPA Principle 6 and GDPR Articles 12-22 – data subject rights	Yes	Directions will be issued to ensure 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 DPA Principle 7 and GDPR Principle 6 - security	Yes	Directions will be issued to ensure 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 DPA Principle 8 and GDPR Article 24 - 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.

7. 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 collection, sharing and use of data held by GP contractors.	1	Directions and data sharing agreements will be prepared to obligate and incentivise that data protection requirements are properly complied with.	Reduced


8. 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	Complete data sharing agreements and related Directions.	Richard Foggo, Primary Care Division

9. Authorisation and publication

I confirm that the impact of applying this policy has been sufficiently assessed against the needs of the privacy duty:

<p>Name and job title of a IAO or equivalent</p>  <p>Richard Foggo Head of Primary Care</p>	<p>14 February 2018</p>
--	--------------------------------