Community Health & Social Care Directorate
Primary Care Division

The Scottish Government
Riaghaltas na h-Alba

Addresses

For Action
Chief Executives NHS Boards
Chief Officers for Health and Social Care Partnerships
Caldicott Guardians
eHealth leads
Information Governance Leads
GP Practices
For information
Scottish General Practitioners Committee
Primary Care Leads NHS Boards

Policy Enquiries to:
Joseph McKeown
Primary Medical Services
1 East Rear
St Andrew's House
Edinburgh
EH1 3DG

Tel: 0131-244 4928
Joseph.McKeown@gov.scot

27 November 2019

Dear colleague

JOINT CONTROLLER AND INFORMATION SHARING AGREEMENT FOR HEALTH BOARDS AND GP CONTRACTORS

1. The document accompanying this circular is a template Joint Controller and Information Sharing Agreement ("ISA") for use by GP contractors and contracting Health Boards to support the safe and appropriate sharing of patient information. It has been developed and agreed by the Scottish Government, BMA and representatives of Health Boards with technical input from Scottish Clinical Information Management in Practice, and NHS National Services Scotland.

2. The most comprehensive record of a person's health is kept within the GP record. Safe and appropriate information sharing across healthcare settings is essential for good care. Good information governance and the regulatory framework which underpins it can be used to promote safer and more effective care through appropriate information sharing across healthcare settings.

3. To support this, the BMA and Scottish Government agreed that the 2018 GP Contract would include better recognition that GP contractors and their contracting Health Boards are the joint controllers of the personal data held within GP patient records. The National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018 and the National Health Service (Primary Medical Services Section 17C Agreements) (Scotland) Regulations 2018 came into force in 2018 to implement the new contract and require the Health Board and the GP contractor to include within their contract a term that requires them to act jointly as data controllers in relation to the processing of patient records.

4. This work was supported by an Information Sharing Short Life Working Group created in 2017 to clarify the information governance roles, responsibilities and liabilities between Health Boards and GP contractors in relation to the information in GP patient records. The

Group concluded that there was a need for Health Boards and GP contractors to enter into ISAs with each other, and that it would be most appropriate for a national standard template ISA to be co-developed by Health Boards and adjusted to meet the needs of local areas where necessary.

Users of the Information Sharing Agreement

5. The ISA is for use by contracting Health Boards and their GP contractors. It will also assist IT and information governance staff in Health Boards. The document will also be of use to patients seeking further details about how information is shared between their GP practice and Health Board.

Matters covered by the Information Sharing Agreement

6. The ISA is designed to assist Health Boards and GP contractors to determine in a transparent manner their respective responsibilities for complying with data protection legislation.

7. The ISA sets out the parties' respective responsibilities as joint controllers of the personal data contained within the patient records held by the GP Contractor.

8. The ISA also sets out the rules to be applied by the Health Board and the GP contractor when sharing personal data with each other, including with staff employed, contracted or engaged by either party, to enable the delivery of NHS services to the GP contractor's patients.

9. Information relating to the provision by the GP contractor of non-NHS services ('private work') are outside the scope of the ISA. GP contractors are expected to meet their requirements under Data Protection legislation for non-NHS services.

10. The ISA is designed to be a comprehensive source of support and it refers to a wide range of the most-common considerations for information sharing. However it cannot cover every possible situation that may arise. Where situations arise that are not covered in the ISA both parties should seek further appropriate advice.

Actions

11. Health Boards are requested to ensure that their information governance leads and primary medical services contractors are aware of this document.

12. Health Boards should seek to agree a joint controller and information sharing agreement with their primary medical services contractors using the attached template ISA.

Enquiries

13. In the instance of any enquiries on this circular please contact Joseph McKeown.

Aidan Grisewood, Deputy Director, Primary Care Division
Community Health and Social Care Division

Joint Controller and Information Sharing Agreement

between

NHS Scotland Health Boards and General Practitioner Contractors

Contents

*[**Guidance Note**: This document, including Appendices 1 to 7, shall be referred to throughout as "the Agreement". For ease of reference, capitalised terms used in this Agreement are defined and/or explained in Appendix 1 – Glossary of Terms**]***

1.0 Introduction

The sharing of information between the people who are involved in the care of Patients is increasingly important to the safe and effective delivery of health and social care. Information sharing is vital to the operation of a comprehensive and integrated health and social care system which has patients at its centre.

In the context of NHS Scotland, the development of extended primary care multi-disciplinary teams consisting of GP Contractors, Health Board employed staff and other parties contracted to either a GP Contractor or a Health Board, requires appropriate sharing of information in order to secure the best care for Patients.

The new GMS Contract and PMS Agreements both recognise GP Contractors are not the sole controllers of Personal Data within the patient records held by the GP Contractor. They are joint controllers along with their contracting Health Board.

The principal reasons why GP Contractors and Health Boards are joint controllers are described in the letter issued from ICO Scotland (provided in Appendix 7) to the Chair of Information Sharing Short Life Working Group in 2017.

These reasons include an acknowledgement that, where agreed, employed, contracted, or engaged Health Board staff may access and amend Personal Data held within the GP Record in the process of delivering NHS services, and in those circumstances GP Contractors may not have sole effective control of how Personal Data is processed.

Therefore, Health Boards and GP Contractors must, as joint controllers, determine in a transparent manner their respective responsibilities for complying with Data Protection Legislation. The GMS Regulations (Schedule 6, paragraph 65(2)(b)) and the PMS Regulations (Schedule 1, paragraph 34(6)(b)) respectively state that GMS contracts and PMS Agreements must include *"a term that requires the Health Board and the contractor to act jointly as data controllers in relation to the processing of patient records."*

This Agreement is designed to support GP Contractors and Health Boards set out their Joint Controller arrangements. It also sets out where other rules, codes of practice and guidance is available to support the Health Board and a GP Contractor when sharing information with each other to enable the delivery of NHS Services to the GP Contractor's Patients.

A Data Protection Impact Assessment has been completed in connection with this agreement. It has been carried out in relation to the sharing of Personal Data by GP Contractors and Health Boards for the purposes of the delivery of NHS Services. Any preparatory work, actions and measures taken as a result of that Data Protection Impact Assessment, as well as any arrangements to minimise the impact of the sharing

of information on the rights of the Patients concerned, are set out in the Data Protection Impact Assessment itself.

2.0 Parties to the Agreement

Legal name of Parties to ISA	Short name of the party	Head Office address	ICO Registration
GP Contractor as per Section 22 – Sign Off "Joint Controller Agreement Form"	GP Contractor	As referred to in Section 22 – Sign Off "Joint Controller Agreement Form"	As referred to in Section 22 – Sign Off "Joint Controller Agreement Form"
{INSERT HEALTH BOARD}	{INSERT SHORT NAME}	{INSERT ADDRESS}	{INSERT REGISTRATION NUMBER}

Both Parties to this Agreement are public authorities for the purposes of the General Data Protection Regulations 2018 (GDPR). The GP Contractor is a public authority only in respect of information relating to the provision of NHS Services under its GP Contract.

The GMS Regulations (Regulation 14) and PMS Agreement (Regulation 15) set out the requirement for Contracts and Agreements to set out the names of the parties to the contract and addresses to which official correspondence should be sent.

2.1 Data Protection Officers

Both Parties are required by current Data Protection Legislation to designate a Data Protection Officer (DPO). The Parties may jointly designate a DPO. Where the Parties have not jointly designated a DPO, each Party will inform the other Party in writing of the contact details for its DPO. Each Party will notify the other in writing of any change to those details.

3.0 Scope of the Agreement

This Agreement sets out the Parties' respective responsibilities, as set out in Data Protection Legislation, as Joint Controllers of the Personal Data contained within the patient records held by the GP Contractor in respect of the GP Contractor's and Health Board's attendance on and treatment of the GP Contractor's Patients.

This Agreement also sets out the rules to be applied by the Health Board and the GP Contractor when sharing Personal Data with each other, including with staff employed, contracted or engaged by either party, to enable the delivery of NHS Services to the GP Contractor's Patients.

Information relating to the provision by the GP Contractor of services outside of NHS Services ('private work') are outside the scope of this Agreement. GP Contractors are

expected to meet their requirements under Data Protection Legislation for non-NHS Services.

4.0 Business and Legislative drivers for the processing

4.1 Business drivers

The delivery of Primary Medical Services (the services provided under a GP Contract) is increasingly a collaborative endeavour between GP Contractors and other professionals, employed, contracted or engaged by Health Boards, as part of a primary care multi-disciplinary team. The sharing of information between members of primary care multi-disciplinary teams is essential for the safe and effective delivery of Primary Medical Services.

All clinicians are subject to professional obligations regarding information sharing. In particular, doctors, including GP Contractors should have regard to the General Medical Council's "Confidentiality: Good Practice in handling patient information" Guidance dated 25th April 2017.

Paragraph 26 of that guidance stresses the importance of information sharing:

"Appropriate information sharing is an essential part of the provision of safe and effective care. Patients may be put at risk if those who provide their care do not have access to relevant, accurate and up-to-date information about them. Multidisciplinary and multi-agency teamwork is also placing increasing emphasis on integrated care and partnership working, and information sharing is central to this, but information must be shared within the framework provided by law and ethics."

Further, the seventh Caldicott principle, set out in the "Information Governance Review" of March 2013 states:

"The duty to share information can be as important as the duty to protect patient confidentiality."

4.2 Legislative drivers

Duties to provide NHS Services are conferred on Health Boards by or under the National Health Service (Scotland) Act 1978. In particular, an important driver for the sharing of information is the requirement under section 2C of the NHS Act for Health Boards to provide, or secure the provision of, Primary Medical Services.

These Primary Medical Services are provided by GP Contractors to their Patients under a GMS Contract or PMS Agreement, the terms of which are regulated by the GMS and PMS Regulations respectively. For each GP Contractor, the legislative drivers for sharing information are set out in the GMS or PMS Regulations and reflected in their GP Contract.

These Primary Medical Services include (where necessary and appropriate) the referral of Patients for other services under the NHS Act and liaison with other health care professionals involved in the treatment and care of Patients.

The GMS and PMS Regulations have specific provisions which describe component types of service. Information for any of these component types may need to be shared for full service delivery.

These regulatory drivers inform seven core purposes which information is processed for. These purposes can be realised by use of any or all of nine formal categories of information. Specific provisions of the GMS and PMS regulations, the core purposes, and the information categories are detailed in Appendix 2 and 3.

5.0 Purpose(s) of the processing, including information sharing

The purpose of the Processing and of the sharing of information covered by this Agreement is to deliver NHS Services.

This purpose includes, but is not limited to, the following sub-categories:

a) medical diagnosis of, or provision of healthcare to, Patients, including registration, prescribing, record-keeping and certification for Direct Care;
b) audit and review of NHS Services, including where it is reasonably required in connection with the GP Contract; and
c) the planning, including workforce planning as set out in the GMS and PMS Regulations, and management of health and social care services.

6.0 Lawful basis for processing, including information sharing

Without detriment to any other legal bases that may be applicable (e.g. vital interests, etc.), the following are the core legal bases for each of the Parties Processing the Personal Data covered by this Agreement. Any other applicable lawful basis will be detailed in the privacy notice.

Relevant GDPR Articles	
6(1)(e) the processing is *necessary* for the performance of a task carried out in the public interest or in exercise of official authority vested in the Controller(*)	**9(2)(h)** the 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 on the basis of law, or pursuant to contract with a health professional AND … is subject to: **9(3)** the requirement to process by or under the responsibility of a professional subject to the obligation of *professional secrecy* under law or rules established by national competent bodies, or by another person also subject to an obligation of secrecy under law or rules established by national competent bodies(*)(**) Note: This also satisfies the condition in section 10(2) of the Data Protection Act 2018 for the processing of data concerning health. This condition is met if the processing is necessary for health or social care purposes.

*Although the GP Contractor is performing activities pursuant to and in accordance with the contractual obligations set out in the GP Contract, from a data protection perspective the GP Contractor is performing such activities in the public interest. The Health Board, on the other hand, is performing activities both in the public interest and also in the exercising of official authority vested in the Health Board by virtue of the GMS and PMS Regulations and / or the NHS Act.[1]

**All engaged staff must abide by contractual terms and also the Protecting Patient Confidentiality: NHS Scotland Code of Practice.

Non-clinical staff who do not have an obligation of professional secrecy are covered by the common law duty of confidentiality (see Section 9).

7.0 The Data Protection Principles

The Parties have entered into this Agreement to assist them with Processing Personal Data in accordance with the data processing principles set out in the General Data Protection Regulations. Those principles are, in summary that Personal Data shall be:

(a) processed lawfully, fairly and in a transparent manner;
(b) collected for specified, explicit and legitimate purposes;
(c) adequate, relevant and limited to what is necessary;
(d) accurate and, where necessary, kept up to date;
(e) 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; and
(f) processed in a manner that ensures appropriate security of the Personal Data.

Furthermore, accountability is central to GDPR: the GP Contractor and the Health Board are responsible for compliance with these principles and must be able to demonstrate this to Patients and the appropriate supervisory authority.

8.0 The Caldicott Principles

The Parties acknowledge that the Caldicott Principles must be applied to the Processing of Personal Data to ensure that the information is only shared for justified purposes. The Caldicott Principles are:

1) justify the purpose(s) for using confidential information;
2) only use it when absolutely necessary;
3) use the minimum that is required;
4) access should be on a strict need-to-know basis;
5) everyone must understand his or her responsibilities;
6) understand and comply with the law; and
7) the duty to share information can be as important as the duty to protect patient confidentiality

[1] DPA 2018 Section 8(c)

9.0 The Common Law Duty of Confidentiality

The Parties also acknowledge that they owe a duty of confidentiality to the GP Contractor's Patients. The General Medical Council describes the duty of confidentiality in the following terms:

"Information acquired by doctors in their professional capacity will generally be confidential under the common law. This duty is derived from a series of court judgments, which have established the principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances. This means a doctor must not disclose confidential information, unless there is a legal basis for doing so."

The common law duty of confidentiality is the general position that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's agreement.

It is generally accepted that the common law allows disclosure of confidential information relating to a Patient if:

a) the Patient consents;
b) it is required by law, or in response to a court order; or
c) it is justified in the public interest.

The common law cannot be considered in isolation. Even if a disclosure of confidential information is permitted under the common law, the disclosure should still satisfy the requirements of Data Protection Legislation and guidance in place to support patients, clinicians and Health Boards manage confidentiality appropriately. In addition to the GMC guidance *Confidentiality: Good Practice in Handling Patient Information*, further sources of guidance are the *Charter of Patient Rights* (2019), which sets out the right of patients to privacy and for their personal health information to be protected when using NHS services.

10.0 Description of the information covered by this Agreement

10.1 Information subject to the Joint Controller arrangements

The Parties are the Joint Controllers of the Personal Data held on GP patient records for the purpose of the GP Contractor's and the contracting Health Board's attendance on and treatment of the GP Contractor's patients. These records also include information recorded by staff employed, contracted or engaged either by the GP Contractor or the Health Board. This may include health care professionals who provide clinical services to the GP Contractor's patients, as well as administrative staff.

10.2 Information to be shared by the Parties

The information to be shared by the Parties consists of information to enable the provision of NHS Services to the GP Contractor's Patients by the Parties and by other NHS organisations, NHS dental, ophthalmic or pharmacy contractors.

10.3 Common factors to the information covered by this Agreement

The information covered by this Agreement contains Personal Data relating to Patients. It will contain the special categories of Personal Data set out in Article 9 of GDPR, including data concerning health, genetic data and data revealing racial or ethnic origin.

The information may also include Personal Data relating to third parties where that is relevant to the provision of NHS Services to the GP Contractor's Patients. Examples of this include the names and contact details of Patients' next of kin and / or carers. Specific categories of the information covered by this Agreement are set out in Appendix 3 (Categories of data).

The information will be kept within records of the Parties' attendance on and treatment of the GP Contractor's Patients. These records will be kept on paper forms supplied by the Health Board or using electronic patient records held on Clinical Information Systems provided or approved by the Health Board, including but not limited to those set out in Appendix 5 (Information Systems used in GP Practices).

10.4 Proportionate Information Sharing

Particular types of information are required to be processed for specific Primary Medical Services. The information shared must be proportionate, relevant and appropriate for the purpose required, and not excessive as agreed between parties.

10.5 Methods of Information Sharing

The principal means used by the Parties will be via a GP's Clinical Information Systems which use Role-based Access Controls (RBAC) to control the sharing of information. More detail is provided in Appendix 4 (Role-Based Access Controls: an Overview) and Appendix 5 (Information Systems used in GP Practices) all of which use some form of RBAC, except most of those in section 3d "non-clinical."

Information sharing will also take other forms including, for example, written, verbal, data extracts and reports.

11.0 Responsibilities for Processing

The Parties agree that each Party will have lead responsibility for the information, including Personal Data, which it creates and processes for the purposes of the delivery of NHS Services. Thus:

- the GP Contractor has lead responsibility for the information created and processed by its staff or by any party employed, contracted or engaged by it.

- the Health Board has lead responsibility for the information created and processed by its staff or by any party employed, contracted or engaged by it.

Decisions to share data between the Parties should be agreed between the Parties as set out in Section 21 'Decision Making Arrangements'.

The Parties acknowledge that where one Party lawfully shares information, including Personal Data, with the other Party, the Party which shares the information is not responsible for the onward Processing of that information by the other Party once received.

The Parties acknowledge that the delivery of services which are not NHS Services may require information sharing which is outside the scope of this Agreement.

11.1 Authorisation of access to Personal Data

It is the responsibility of each party to ensure the correct authorisation and training are in place for individuals they have employed, contracted or engaged,. Where the party does not have lead responsibility, the other party must be satisfied those arrangements are in place.

In particular, the GP Contractor must ensure, and keep a record of doing so, that it: (a) has verified the identity of each person that presents himself or herself at the GP Contractor's premises for the purposes of processing Personal Data; and (b) has satisfied itself that such a person is authorised by the Health Board, or an organisation which has an agreement with the Health Board, *before* providing that person with access to any Personal Data.

11.2 Third Party Disclosure

Where a Party is asked to carry out Processing of Personal Data it has acquired from the other Party, which may include disclosure to a third party, there should be an appropriate legal basis. Examples include:

- the maintenance of the physical and/or mental health of the Patient who is the subject of the information;
- satisfying a Party's duty to provide information as required by Directions from Scottish Ministers, or by a statutory regulator;
- complying with a legal obligation to share such information; or
- necessary for the preparation of a medical report where the Patient has consented.

12.0 Privacy Notices (Transparency)

The Parties agree that a tiered approach to transparency will be followed, in line with the ICO recommendations.

As set out in the GMS and PMS Regulations, the Health Board must provide privacy notices to the GP Contractor. The GP Contractor must check the accuracy of the notice. The GP Contractor will be responsible for amending the privacy notice to ensure that any local GP contractor arrangements are reflected in it.

The GP Contractor will use the privacy notice to inform its Patients about how their Personal Data is processed by the Parties. The ways in which the GP Contractor will do this will include:

- providing the privacy notice to Patients when they register with the GP Contractor;
- displaying a copy in the practice reception area;
- publishing a copy on the GP Contractor's website (if it has one); and
- providing a copy to all Patients who request one.

The Health Board will publish a privacy notice on its website.

The Parties agree that further privacy notices may be produced as required for particular methods of processing in order to ensure appropriate transparency with Patients. The Parties will take the advice of their respective DPOs in this regard.

13.0 Accuracy of the information

As per Article 5(1)(d) of GDPR, both Parties are responsible for ensuring Personal Data is accurate and, where necessary, is up to date.

The Parties will ensure all staff using information shared by the other Party understand the limitations of such extracts and take all reasonable steps to confirm the accuracy of the information. This will involve confirming the accuracy of the information with the Patient where possible.

It is the responsibility of both Parties to ensure that their staff know how to respond to the identification of an actual or possible inaccuracy in information. The response to an inaccuracy should be managed by each Party according to a policy implemented and adhered to by that Party, with procedures based on professional guidance.

It is the responsibility of the Party identifying the inaccuracy to ensure that the Controller of the record from which the information originated is informed about the inaccuracy.

Where a correction to a record in a Clinical Information System is required, a process such as those described in the Good Practice Guide for Electronic Records 2011 (or any update to it) should be followed.

14.0 Security

Both Parties have agreed to comply with Health Board data security, personal data and IT policies.

The Health Board is responsible for providing, maintaining and, where necessary, upgrading the Clinical Information Systems used by the GP Contractor for providing services under the GP Contract. The Health Board is also responsible for providing any telecommunication links between the GP Clinical Information Systems and the systems used by the Health Board or other NHS organisations. The Health Board will ensure the technical security of GP Clinical Information Systems and the telecommunication links it provides to the GP Contractor (GMS Regulations, Schedule 6, Part 5, Paragraph 71; PMS Agreement, Schedule 1, Part 5, Paragraph 39).

The GP Contractor is responsible for ensuring that its staff use such GP Clinical Information Systems, at all times, in accordance with all relevant IT security

frameworks, user manuals and licence terms (GMS Regulations, Schedule 6, Part 5, Paragraph 66; PMS Agreement, Schedule 1, Part 5, Paragraph 35 (1)).

The Health Board will notify the GP Contractor of its data security, personal data and IT policies and will notify it of any changes to the same as soon as practicable (GMS Regulations, Schedule 6, Part 5, Paragraph 67; PMS Agreement, Schedule 1, Part 5, Paragraph 35 (2)).

The GP Contractor is responsible for complying with the Health Board's current policies concerning data security, personal data or IT security notified by the Health Board to the contractor (GMS Regulations, Schedule 6, Part 5, Paragraph 66 (b); PMS Agreement, Schedule 1, Part 5, Paragraph 35 (1b)). This should include ensuring the physical security of electronic devices used by its staff for Processing Patient information and of any of the GP Contractor's physical files containing Patient information, as well as responsibility for the physical security at its premises (unless otherwise agreed in writing with the Health Board).

Both Parties will ensure that any person under its direction who has access to patient records has undergone adequate data protection training ((GMS Regulations, Schedule 6, Part 5, Paragraph 66 (e), and 67 (e); PMS Agreement, Schedule 1, Part 5, Paragraph 35(1)(f) and (2)(f)).

They should ensure Personal Data is only Processed by individuals who have either a professional or a contractual duty of confidentiality.

15.0 Personal Data Breaches

Each Party will ensure that the other Party is notified of any Personal Data breach, or significant information security risks, affecting the information subject to the Joint Controller arrangements as soon as practicable, and within one working day of becoming aware of the same, at the latest.

The DPO of the Party responsible for the Breach, (as determined pursuant to section 10), will assess and consider whether the Personal Data breach requires to be reported to the ICO. A log of Personal Data breaches will be maintained by the DPO of the responsible Party.

The Parties will, where appropriate, work together to rectify any such Personal Data breach or mitigate any such risk to information security, including notification to affected individuals if required.

16.0 Information Asset Registers

Article 30 of GDPR requires Controllers to maintain a record of Processing activities under its responsibility. A method of delivering this is through the completion of an Information Asset Register.

The Parties agree that they will each maintain separate Information Asset Registers as set out in Article 30.

The Health Board will provide guidance on Information Asset Registers to the GP Contractor (GMS Regulations, Schedule 6, Part 5, Paragraph 67(b)).

The Health Board will provide a template Information Asset Register to the GP Contractor (GMS Regulations, Schedule 6, Part 5, Paragraph 67 (b)).

The Health Board will provide the relevant information regarding all Clinical Information Systems which it provides to the GP Contractor for the purposes of the delivery of NHS Services. This is to allow the GP Contractor to include that information in its Information Asset Register. See Appendix 5 (Information Systems used in GP Practices) for an overview.

17.0 Training

Both Parties will ensure that all of their employees, contracted or engaged staff who have access to information about the GP Contractor's Patients have undergone adequate data protection training.

The Health Board will make available appropriate data protection training to the GP Contractor and its employees.

Both Parties will ensure that their employees and other persons under their direction who can create, update or delete Personal Data are adequately trained: (a) in records keeping; (b) on the Clinical Information Systems that they are using; and (c) in any specific data recording requirements that are relevant to their role.

18.0 Data retention

Data must be retained in accordance with the Scottish Government Records Management NHS Code of Practice (Scotland).

Data which is no longer required must be disposed of in accordance with the Scottish Government Records Management NHS Code of Practice (Scotland) and the NHS Scotland Information Security Policy Framework.

19.0 Individuals Rights

The Parties acknowledge that the current Data Protection Legislation provides Data Subjects with a number of rights in respect of their Personal Data. As a result, each Party's privacy notice must inform Patients how they can exercise their rights under Data Protection Legislation.

The most commonly used rights for GP Contractors are set out below, but others described in current Data Protection Legislation may be used and arrangements for all rights should be set out in the Privacy Notice.

19.1 Subject Access Requests

The GP Contractor is responsible for responding to requests made to it by Patients for access to their Personal Data held by the GP Contractor.

The Health Board is responsible for responding to requests made to it by Patients for access to their Personal Data held by the Health Board.

19.2 Rights related to automated decision making, including profiling

The Parties acknowledge that Automated Decisions are not currently relevant to subject matter of this Agreement.

In the event of the development of new forms of Processing that involve Automated Decisions, the Parties agree that they will carry out a DPIA before making any decision to adopt the new form of Processing.

19.3 Direct Marketing

The Parties acknowledge that no Direct Marketing is involved in this Agreement. In the event of Direct Marketing being required, the Parties will carry out a DPIA. The Parties will ensure that appropriate mechanisms are in place to allow Patients to opt in to the Direct Marketing. Any such arrangements must be documented in a variation to this Agreement.

20.0 International transfers of personal data

The Parties will not as standard transfer the Personal Data of patients outside of the UK or European Economic Area for the purposes of the delivery of NHS Services.

Where it is proposed to transfer Patients' Personal Data to a country within the European Economic Area or another country, each Party will individually consider whether a DPIA is necessary, and this may include receiving advice from the relevant DPO, before making a decision on whether to agree to the proposal. Any transfer shall be compliant with current Data Protection Legislation.

Each Party will individually assess the risk of clinically urgent or "one off" transfers of Personal Data for Direct Care, with patient consent as appropriate, before making a decision.

21.0 Decision Making Arrangements

The decision-making process in respect of Joint Controller arrangements must be agreed locally. This should determine where individual GP Contractors should be consulted by default and/or where the GP Subcommittee can act as a representative of one or more contractors where said GP Contractors have agreed to delegate responsibility for decision making to that Committee.

The Health Board and the GP Contractor will make decisions in accordance with the latest guidance from the ICO, and follow a data protection by design and default approach in compliance with the Data Protection Legislation.

The Parties agree that a DPIA will be carried out where there is a proposed change to the manner of Processing of Personal Data for the purposes of this Agreement and the proposed change is likely to result in a high risk to the rights of Patients.

The Parties will take the advice of their DPOs on the necessity of carrying out DPIAs.

The Parties agree that where such a proposed change will apply to more than one GP Contractor, they (or its GP Subcommittee) will review any DPIA before the Parties make a decision on whether to agree to the proposed change.

Any DPIA will also be reviewed by the Parties' DPOs before the Parties make a decision on whether to agree to a proposed change.

The Parties will update their own Information Asset Register accordingly when a new DPIA is completed or an existing one is reviewed.

The Parties acknowledge that any actions and countermeasures agreed as part of a DPIA must be implemented by the responsible Party. Deadlines and follow up to progress on those actions will be established as part of the DPIA review process.

22.0 Monitoring, review and continuous improvement

This Agreement will be reviewed by the Health Board and the GP Contractor every three years or as required by either Party due to a significant change of circumstances. The Health Board and the GP Contractor will then agree any necessary amendments, if any.

23.0 Sign Off

INSERT NHS BOARD LOGO

JOINT CONTROLLER AGREEMENT FORM

The undersigned agree to the details recorded in this Joint Controller and Information Sharing Agreement; and are committed to the ongoing monitoring and review of the Joint Controller arrangements and the scope, purpose and manner of the information sharing.

Name of Health Board		
Authorised signatory, e.g. Caldicott Guardian, SIRO, Chief Executive	Title and name	
	Role	
Signature and date		

Name of GP Contractor	
Address	
Practice Code	
ICO Registration Number	
Authorised signatory	

By signing this form you are acknowledging the Joint Controller arrangements and data sharing principles and rules detailed in the “Joint Controller and Information Sharing Agreement between NHS Scotland Health Boards and General Practitioner Contractors”. Joint Controller arrangements are contractual requirements specified in the GP Contract Regulations applicable to the GP Contractor (GMS Regulations, Schedule 6, Part 5, Paragraph 65; PMS Agreement, Schedule 1, Part 5, Paragraph 34 (6)).

Appendix 1 Glossary of Terms

Term	Definition
Automated Decision	A decision based solely on automated processing, including profiling, which produces legal effects concerning a Patient or similarly significantly affects him or her. See GDPR recital 71-75.
Clinical Information Systems	Any integrated information management and technology systems used by the contractor for provision of services under the contract and any telecommunication links between these systems and the systems used by the Health Board, in accordance with any relevant guidance (including standards) issued from time to time by the Scottish Ministers.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (see GDPR (Article 4(7)).
Data Protection Legislation	(i) The GDPR and any applicable national implementing laws as amended from time to time; (ii) the DPA 2018 to the extent that it relates to the Processing of Personal Data and privacy; and (iii) any other law in force from time to time with regards to the Processing of Personal Data and privacy, which may apply to either party in respect of its activities under this Agreement.
Data Subject	Defined in Article 4 of GDPR as 'an identified or identifiable natural person'.
Direct Care	Health activities provided by individually-identifiable healthcare staff who are accountable either under a professionally regulated duty of care or by specific contractual terms, for one or more Patients when they are either: • ill, with conditions from which recovery is generally expected, • terminally ill, or • suffering from chronic disease, • well, and individually responding to contacts from screening, preventive or follow-up services, over a period of time understood between each Patient and Health staff delivering these services.
DPA 2018	The Data Protection Act 2018.
Data Protection Impact Assessment (DPIA)	An assessment undertaken in accordance with Article 35 of the GDPR.
Data Protection Officer (DPO)	The role to be designated and carried out pursuant to Articles 37 to 39 of the GDPR.
General Data Protection Regulations (GDPR)	The General Data Protection Regulation (Regulation (EU) 2016/679).

GMS Regulations	The National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018.
GP Contract	A contract entered into under the GMS Regulations or PMS Agreement.
GP Contractor	A person or organisation which has a GP Contract with a Health Board to provide Primary Medical Services.
GP Subcommittee	A delegated subcommittee of the statutory Area Medical Committee as enabled by the National Health Service (Scotland) Act 1978, Part 1, section 9.
Health Board	A Board constituted pursuant to the National Health Service (Scotland) Act 1978, Part 1, section 2.
Information Commissioner's Office (ICO)	The United Kingdom's supervisory authority for the purposes of Articles 51 of GDPR.
Information Asset Register	A register of information specifying relevant hardware, software, functions, locations, owner, and Processing, e.g. access, sharing and retention.
Personal Data Breach	Defined in Article 4 of GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Joint Controller	Defined in Article 26 of GDPR as 'two or more controllers jointly determine the purposes and means of processing'
NHS Act	The National Health Service (Scotland) Act 1978).
NHS Scotland	The National Health Service in Scotland.
NHS Services	Services which are provided under the NHS Act.
Party / Parties (to the agreement)	The GP Contractor and contracting Health Board which have agreed to enter into this Agreement.
Patient	Patient has the same meaning as in the GMS and PMS Regulations. The GMS Regulations (regulation 3) define patient as: (a) a registered patient; (b) a temporary resident; (c) persons to whom the contractor is required to provide immediately necessary treatment under regulation 18(6) or (8) respectively; and (d) any other person to whom the contractor has agreed to provide services under the contract. The PMS Regulations (regulation 3) defines patient as

	"(i) a registered patient; (ii) a temporary resident; and (iii) persons to whom the provider is required to provide immediately necessary treatment under paragraph 1(5) or 1(7) of schedule 2 respectively; and (b) in all cases any person (or, where the provider has a provider's list of patients, any other person) to whom the provider has agreed to provide services under the agreement."
Personal Data	Defined in Article 4 of GDPR as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.
PMS Regulations	The National Health Service (Primary Medical Services Section 17C Agreements) (Scotland) Regulations 2018.
Primary Medical Services	Those NHS Services provided, or to be provided, under a GP Contract.
Processing	Defined in Article 4 of GDPR as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.
Role-based Access Control (RBAC)	A method of regulating access to computer or network resources based on the roles of individual users within an organisation operating with appropriate information governance checks and controls. This can be used by Clinical Information Systems to link individual health staff permissions to the data required for a specific task, which commonly uses combinations of Create, Read, Update or Delete functions for the processing of stored data. This is described in more detail in Appendix 4.

Appendix 2 Map of Primary Medical Services, Purposes and Data Categories

This list is intended to help parties to this agreement set out the purposes of processing information.

We have organised these into Data Categories. These are defined, and expanded with common examples from Primary Care, in Appendix 3.
Any or all of these Data Categories may be required for any Purpose e.g. data in

- category a) (identifying people) is required for most types of service delivery.
- category i) (communications) is required for status tracking of any service types.

GMS Regulations Reference	PMS Agreement Reference	Description of Primary Medical Service	Principal Purpose	Data Category
Schedule 6, Part 2, Paragraph 13	Schedule 2, Part 2, Paragraph 8	Temporary Residents	Direct Care	any
Part 5, Paragraph 18	Part 4, Paragraph 13	Essential Services	Direct Care	any
Part 5, Paragraph 19	Part 4, Paragraph 14	Additional Services	Direct Care	any
Part 5, Paragraph 25	Part 5, Paragraph 20	Certificates	Certificates	a h
Schedule 6, Part 5, Paragraph 68(1)	Schedule 1, Part 5, Paragraph 36 (1)	Contractor must keep adequate records	Records	any
Schedule 6, Part 5, Paragraph 68(2)	Schedule 1, Part 5, Paragraph 36 (2)	Include reports from others	Records	any
Schedule 6, Part 5, Paragraph 68(4)	Schedule 1, Part 5, Paragraph 36 (4)	Audit trail access	Audit & Review	a h
Schedule 6, Part 5, Paragraph 68(5)	Schedule 1, Part 5, Paragraph 36 (5)	Transfer record on death, de-registration	Registrations	a b e
Schedule 6, Part 5, Paragraph 69(3)	Schedule 1, Part 5, Paragraph 37	Share with HB for direct care	Direct Care	any
Schedule 6, Part 5, Paragraph 69(3)	Schedule 1, Part 5, Paragraph 37	Share with HB as contractual	Audit & Review	a e h
Schedule 6, Part 5, Paragraph 69(3)	Schedule 1, Part 5, Paragraph 37	Share with HB for service management	Planning	d h
Schedule 6, Part 5, Paragraph 75(1)	Schedule 1, Part 5, Paragraph 37	Inquiries	Audit & Review	a e h

GMS Regulations Reference	PMS Agreement Reference	Description of Primary Medical Service	Principal Purpose	Data Category
Schedule 6, Part 5, Paragraph 76(1)	Schedule 1, Part 5, Paragraph 43	Medical Officers	Direct Care	a e
Schedule 6, Part 5, Paragraph 78	Schedule 1, Part 5, Paragraph 45	Address or other status changes	Registrations	a b
Schedule 6, Part 3, Paragraph 38	Schedule 1, Part 3, Paragraph 11	Prescribing	Prescribing	a g
Schedule 1, Paragraph 2	Schedule 3, Paragraph 2	Cervical Screening	Direct Care	a e h
Schedule 1, Paragraph 3	Schedule 3, Paragraph 3	Contraceptive Services	Direct Care	a e h
Schedule 1, Paragraph 4	Schedule 3, Paragraph 4	Vaccinations	Direct Care	a g h
Schedule 1, Paragraph 5	Schedule 3, Paragraph 5	Childhood Vaccinations and Immunisations	Direct Care	a g h
Schedule 1, Paragraph 6	Schedule 3, Paragraph 6	Child Health Surveillance	Direct Care	a e h
Schedule 1, Paragraph 6	Schedule 1, Paragraph 7	Maternity Medical Services	Direct Care	a e g h

Appendix 3 Categories of Data

Based on categorised index at HL7 FHIR R4 Resources

Data category	Description of Data	Primary Care examples	Personal Data
BASE			
a) Individuals	About or identifying people	Patients, practitioners, third parties; and associated data such as roles and groupings	Yes
b) Entities	About or identifying things	Organisations e.g. general practices, hospitals, departments; medicines, devices, materials, equipment and supplies	No
c) Workflow	To support or define processes and tasks	Appointments and other scheduling, resource management, recalls, tasks	Yes
d) Management	To organise care	Care episode data (not clinical content), alerts and linked knowledge resources, workforce data	Yes
CLINICAL			
e) Summary	Clinical records incl. clinical data codes and narrative; records of procedures, allergies and adverse events; data of third parties relevant to the patient	Problems and disorders, drug allergies, clinical notes, family history, operations and injections	Yes
f) Diagnostics	Observations, measurements, test results, samples and assessments	Vital signs e.g. pulse, blood pressure; haemoglobin, swabs; blood samples; risk scores, self-assessment tools, genomic data	Yes
g) Medications	The ordering, use, administration and dispensing of medications and appliances incl. warnings, recommendations and vaccines	Prescriptions for medicines and items such as dressings, additional instructions/specific advice on use, administrations and dispensing records, immunisations e.g. details / advice for flu	Yes
h) Care Provision	For care planning and to enable cross- organisational care	Palliative care plans, resuscitation wishes, blood pressure targets, goals, falls risk assessments, SCI referrals, social care information	Yes
i) Request / Response	Communications, status tracking	Send and read receipts, data about status of any components of service such as referrals or requests.	Yes

Appendix 4 Role-Based Access Controls

The level of access to information by a member of staff of either Party will depend on that individual's role and the purpose for which that access is required, as listed for example in Appendix 2.

The Parties will use the Role-Based Access Controls within their Clinical Information Systems to control access by all members of their staff to the appropriate and necessary information for each task.

Where one Party shares information with the other Party using Clinical Information Systems, how the recipient carries out the Processing of the information depends on the method and purpose of sharing. The principal types of permissions that a recipient will have are:

Viewing – Read Only
Viewing enables one Party to read information contained in a Clinical Information System, without being able to create, update or delete the information.
Examples of Viewing include:

- A nurse in A&E using a portal viewer to view information about a Patient from the Clinical Information System.
- The GP Contractor using a portal viewer to view a Patient's outpatient appointment schedules.

Direct Access
Direct Access makes information available for both Parties to manage. For this, both Parties' IT systems must provide full Create, Read, Update and Delete permissions for their role. Users are provided with the appropriate permissions for their role.
Examples of Direct Access include:

- health visitors using the GP's Clinical Information System to run an immunisation clinic in the GP Contractor's premises;
- treatment room nurses using a remote login to the GP's Clinical Information System to record a procedure.

Transfer
Transfer refers to the transfer of information between the Parties. Where electronic systems are used, information is transferred between two or more systems and persists in the receiving system or systems. Where paper records are used, a copy of the paper record is transferred from one file to another. Examples include:

- the import of a GP clinical history into a hospital Patient administration system
- a treatment room nurse updating a record in a community Clinical Information System which then sends a copy to the GP's Clinical Information System that is automatically filed.

For the purposes of planning and audit and review, the recipient will normally only require to view the information (Read Only access).

For all other purposes, the recipient system will require full Create, Read, Update and Delete permissions, because of its requirement to synchronise information.

Appendix 5 Information Systems used in GP Practices

Type of Information System	Examples (non-exhaustive list at mid-2019)
1 **GP Clinical^** (Primary*)	Vision / EMIS / Microtest (pending)
2 **Document Management^**	Docman
3 **Other**	
a) Clinical^ mandatory *supplied by NHS*	AMS, CMS, ePharmacy Portal, SCCRS, BOSS, SCI-DC, SCI-GW, SCI-Store, ECS, KIS CHI, SIRS, eLinks, EDT, Partners Order comms: Sunquest ICE / Dart OCM / NPEX/ Plumtree / Cyberlab National Digital Service components: Respect MS Office 365
b) Clinical^ optional *selected by GP Contractor* *supplied by NHS*	Contract & LES mgmt.: Bluebay / MSDi SPIRE, Escro Scottish Therapeutics Utility (STU) Remote Services client support: Attend Anywhere PACS access support: Carestream, Badgernet
c) Clinical^ optional *selected by GP Contractor* *supplied by GP Contractor* *if approved for NHS*	Clinical utilities: Intellisense, DXS, Scriptswitch RAT / INRstar / Bluebay Appt admin: FrontDesk, Jayex Appt check-in: Microtech / Engage Touch Consultn support: AskMyGP / Engage Consult SMS text s/w: iPlato / MJog Phone or SIP call recorders Device monitor s/w: ambulatory BP, ECG etc. Pocket/mobile versions of Clinical Info systems Voice dictation/recognition: Lexacom, DragonDictate
d) Non-clinical *supplied by NHS*	SWAN Single Sign On Remote Access: Citrix, VNC, VPN, Jabber Backup s/w Anti-malware and security s/w Hardware drivers Label printing: Flexatrace Staff security: Little Green Button
4 **Non-NHS**	
Business, Finance optional *supplied by GP Contractor if approved for NHS*	Payroll, finance, HR systems iGPR insurance report generator

- * shows the Primary system as the record of prime entry, and the current default source of truth of data for sharing with other information systems.
- ^ shows “clinical” software that processes patient Personal Data and uses some form of RBAC as locally configured.
- where “/” separates examples of software, a single option is supplied.

Appendix 6 Policies and Procedures that apply for this Agreement

Non exhaustive list of legislation, policies, procedures, standards and codes of practice that apply. Other local policies could also be added to this table.

Title of Policy or Procedure	Document Location
General Data Protection Regulation	https://gdpr-info.eu/
Data Protection Act 2018	www.legislation.gov.uk/ukpga/2018/12/contents/enacted
2018 GMS Regulations	www.legislation.gov.uk/ssi/2018/66/contents/made
2018 PMS Agreement	www.legislation.gov.uk/ssi/2018/67/contents/made
Caldicott Guardian Principles	www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2011/02/nhsscotland-caldicott-guardians-principles-practice/documents/0112733-pdf/0112733-pdf/govscot%3Adocument
Charter of Patient's Rights	www.gov.scot/binaries/content/documents/govscot/publications/publication/2019/06/charter-patient-rights-responsibilities-2/documents/charter-patient-rights-responsibilities-revised-june-2019/charter-patient-rights-responsibilities-revised-june-2019/govscot%3Adocument/charter-patient-rights-responsibilities-revised-june-2019.pdf
General Medical Council's "Confidentiality: Good Practice in handling patient information"	www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality
The Good Practice Guidelines for GP electronic patient records version 4 2011)	www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011
The Information Governance Review, 2013	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
NHS Scotland Code of Practice on Protecting Patient Confidentiality 2012	www.gov.scot/publications/scottish-government-records-management-nhs-code-practice-scotland-version-2-0/pages/8/
NHS Scotland Information Security Policy Framework	www.informationgovernance.scot.nhs.uk/wp-content/uploads/2016/03/IS-Policy-Framework.pdf
National Health Service (Scotland) Act 1978	https://www.legislation.gov.uk/ukpga/1978/29/contents
Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012	www.gov.scot/publications/scottish-government-records-management-nhs-code-practice-scotland-version-2-1-january-2012/

Appendix 7 Letter from Information Commissioners Office Scotland

[Guidance: The following letter was included as an annex to the 2018 Report of the Information Sharing Short Life Working Group]

Dr Lucy Munro
Associate Medical Director (Primary Care)
NHS National Services Scotland Clinical Directorate
Gyle Square
1 South Gyle Crescent
EDINBURGH
EH12 9EB

19 July 2017

Dear Lucy

Data Controllership of Contracted GPs in Scotland

Further to the Short-Life Working Group's request for a formal view on the above matter, I am pleased to provide the following in response to the question of whether GPs in Scotland are correctly designated as data controllers for the patient record, or whether controllership for the patient record would sit better with Health Boards or at least shared with them under a joint Controller relationship.

Background

The Scottish Government has established a short life working group (the Group) to explore the possibility of GPs ceding data controllership in respect of the patient record to Boards. The Information Commissioner's Office (ICO) participates on the Group to provide advice and guidance in respect of data protection matters and has been asked for a formal view on the matter.

GPs in Scotland are currently considered to be data controllers for the patient records they process[2]. However, it has become increasingly difficult for GPs to retain complete control over the patient record, especially when Board employees, such as District Nurses, have full access to the record. Moreover, the various pieces of legislation establishing the legal framework for Boards and GPs vests considerable responsibility on the Board for much of the manner of processing.

[2] For the avoidance of doubt, GPs will always be data controllers in their own right in respect of their role as employers and also for any processing outside that required for the patient record.

Health Boards as data controllers for the patient record

Although decisions about whether to process and what data to process are key in deciding who the data controller is, it is notable that the GPs do not have as much independence as might be expected of a data controller in deciding in what manner the patient record is processed. It is the Boards, rather than the GP practices, that have a considerable amount of control over the manner of the processing. This is arguably more control than a data processor would be permitted to exercise:

1. The National Health Service (Scotland) Act 1978 enables the Scottish Ministers to make directions. The Scottish Ministers have directed, via the Statement of Financial Entitlements 2016-17 in the GMS contract that "NHS Boards, rather than contractors, are responsible for the purchase, maintenance, future upgrades and running costs of integrated IM &T systems for providers of services under GMS contracts, as well as for telecommunications links within the NHS and it is for them to determine the way in which this responsibility is exercised in accordance with any extant national guidance," (Direction 19).

2. The NHS (General Medical Services Contracts) (Scotland) Regulations 2004 (the Regulations) set out that if a GP contractor wishes to keep patient records on computer, it must have the written consent of the Board (Although that consent cannot be withheld if the computer system used is one of two systems accredited by the Scottish Government.)

3. In the event that a GP contractor opts to process patient records manually, the Regulations set out that this must be done on forms provided by the Board. This indicates that the Board is able to exercise some control over what data is recorded in the patient record.

4. Schedule 5, para 66(6)(a) and (b) of the Regulations set out that GP contractors are required to send the complete patient record to the Board where the patient has died or is no longer registered with the contractor. This indicates some data controller responsibility for the Board, at least in the latter case.

5. Increasing numbers of health professionals employed by the Board, such as District Nurses, etc., are accessing and inputting to the patient record.

GPs as data controllers for the patient record

There are a number of arguments to support GPs continuing to be considered data controllers for their patient records:

1. Schedule 5, para 66(2) of the Regulations says:

   "The contractor shall keep adequate records of its attendance on and treatment of its patients..."

   This could engage section 1(4) of the Data Protection Act 1998 (DPA) which says:

   "Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller."

2. The ICO's guidance on data controllers and data processors says in paragraph 12 that this means that "where an organisation is required by law to process personal data, it must retain data controller responsibility for the processing." The Regulations appear to require, via the GMS contract, that GP contractors keep patient records, so they must retain some data controller responsibility for those records.

3. Paragraph 10 of the ICO guidance on data controllers and data processors says that "Activities such as interpretation, the exercise of professional judgement or significant decision-making in relation to personal data must be carried out by a data controller." GPs do exercise professional judgement in terms of what data is required to be recorded and how it is to be used for the care and treatment of the patient in question. In addition, paragraph 19 of that guidance says that "over-arching decisions, for example what the personal data will be used for or what the content of the data is...must only be taken by the data controller." GPs do make those over-arching decisions.

4. Further, paragraph 16 of the ICO guidance on data controllers and data processors sets out a number of decisions that can only be taken by a data controller as part of its overall control of the processing operation. Examples include decisions about the content of the data, whether to disclose the data and to whom, and whether to make non-routine amendments to the data. GPs make decisions about all of these to at least some significant degree.

5. Finally, paragraphs 25+ of the ICO's guidance on data controllers and data processors consider the role of providers of professional services. GPs and/or their practices are regarded as data controllers in respect of the personal data of the patients on their list. They are responsible for the recording and storage and processing of that data for many purposes, not only in order to provide professional advice and care to their patients but also for other purposes such as local healthcare planning, to liaise with other organisations in the health and social care sector. Their professional role in relation to their patients is wide-ranging and ongoing; their professional expertise was required in the first place to obtain the personal data, and they have a continuing role in relation to it – including keeping it up to date as part of patient care.

Conclusion

Boards in Scotland do have some data controller responsibilities for the health record because they have a considerable amount of freedom in deciding the manner of the processing of the patient record. However, GPs will always retain some data controller responsibilities too as they are required by Regulations to keep adequate records of their attendance on and treatment of their patients. GPs also interpret records, and exercise professional judgement and make significant decisions in relation to the personal data held in the patient record. In summary, whilst there is a strong argument for Boards to assume some data controller responsibility for the patient record, it is clear that GPs cannot abrogate or delegate their data controller status for the patient record in respect of those matters previously rehearsed.

Given this determination, it is the view of the ICO that an agreed form of joint data controllership would be a more pragmatic relationship to reflect the current situation.

I trust that the Group finds this helpful.

Kind regards

Maureen H Falconer
Regional Manager - Scotland