draft for consultation, August 2011

Dear Colleague

Proposal to allow Secondary Care to view the GP prescribing information currently available in ECS for medicines reconciliation at the time of admission or when seen after referral

The purpose of this letter is to seek your views on draft guidance that has been prepared, see attached in the form of a letter plus annexe. If responses show sufficient agreement around the content then it is proposed to issue the material more formally in the form of Scottish Government Health Directorates guidance, with any adjustments as necessary.

The issue in question is information sharing between GPs and secondary care clinicians, specifically to allow a patient's GP prescribing information to be made available at the point where the patient attends outpatients or is being admitted. This issue is described in more detail in the attached paper.

In addition to any general comments it would be helpful to have responses to the following questions:

1. Do you agree that providing up to date prescribing information will improve patient care and that using electronic information in a safe and secure manner is a sensible way to enable that improvement?
2. Particularly for patient groups responding to this letter, do you believe that patients expect hospital doctors to be able to check their current prescription?
3. Is the framework set out in the guidance a sound and sufficient basis to proceed?

Replies by 16 September would be helpful.

Yours sincerely

Alan Hyslop
eHealth Strategy
Scottish Government
alan.hyslop@scotland.gsi.gov.uk

Dr Libby Morris
Primary Care Clinical Lead and Chair, ECS Board
Scottish Government
libby.morris@nhs.net

Proposal to allow Secondary Care to view the GP prescribing information currently available in ECS for medicines reconciliation[1] at the time of admission or when seen after referral

Purpose

This guidance letter is to enable appropriate sharing of GP prescribing information in support of elective care medicines reconciliation. It is proposed that in the short term this is done via the Emergency Care Summary with effective safeguards to maintain confidentiality.

While GP practices are responsible under the Data Protection Act for information held solely within the practice, it is GP practices jointly with their NHS Board that are Data Controllers of any shared information such as that held with the Emergency Care Summary (ECS). Both GP practices and NHS Boards therefore need to discuss and agree sharing arrangements, and this paper offers a framework to enable for such agreements.

This proposal builds on the long-established practice of the patient's General Practitioner sending details of prescribing when referring a patient. It would allow the information on prescribing to be updated at the time of the patient being seen rather than having to rely on the out of date information in the original referral letter.

The case for information sharing in support of medicines reconciliation

There is strong evidence of the potential for harm due to medication errors, for example when one prescriber is unaware of other prescriptions.

Currently the main way in which a patient's GP prescription information is shared with secondary care clinicians is through referral letters. However, referral letters may not be up to date by the time the patient is seen at outpatients or is being admitted.

A recent study by NHS Lanarkshire[2] examined the accuracy of medicines information to estimate the risk to safety of patient care and showed that letters were on average 110 days old when the patient was admitted for treatment. In the 24 referral letters examined there were a total of 119 discrepancies in the medications listed by the time of the patient's hospital admission when compared with the information on ECS.

The clinicians who did this study also looked at potential for harm in not having the up to date prescription at the outpatient appointment or admission. They concluded that there may have been some degree of avoidable harm for 23 out of the 305 patients studied, which is a significant finding given the numbers of outpatient appointments and admissions across NHS Scotland.

Currently clinicians in secondary care carry out medicines reconciliation by asking patients/carers about their medication, looking at medications brought in by patients and sometimes by phoning the GP practice. These processes can be a significant challenge as they are often unreliable and time consuming. Moreover the GP

[1] For patients and others unfamiliar with this term, it means the job of compiling an accurate list of patient's current medication for use as they move from one care setting to another

[2] Full report at http://www.scimp.scot.nhs.uk/documents/ECS-Lanarkshire-Final-Report-v-6.0.pdf

practice has no way of knowing that the caller is who they say they are and has a legitimate need to know.

The situation with respect to unscheduled care is better as authorised clinicians working in A&E, Out-Of-Hours GP or NHS24 when GP practices are closed can look up medication and allergy details using the Emergency Care Summary IT system. Patients are asked for their consent for this to be done. This happens some 50,000 times a week, and the fact that it is most unusual for a patient to decline can be taken as evidence that patients see the value of this facility.

How can IT help?

With both GPs and secondary care having computerised patient records it is now possible to make timely information readily accessible to those involved in hospital care of the patient, for example by allowing an electronic check for updates on ECS at the point when the patient attends outpatients or is being admitted. At present this is technically the only way the information can be accessed electronically.

Framework for making this happen

Any information sharing must comply with the law, patient consent and professional guidance. Annexe 1, which has had input from the Information Commissioner's Office, explains in more detail that compliance can be achieved.

A key section in this annexe is section 4 where the various responsibilities on each party are set out. Further guidance is available on what that means by way of various safeguard measures such as management of passwords and so on.

The annexe sets out a framework to enable appropriate information sharing to be agreed by GPs and their NHS Board but this letter is specifically about sharing electronic prescribing data in ECS to support medicines reconciliation. Questions and answers on this may include the following:

> **Can this be done within the law and professional guidance?**
>
> Yes. Plus with respect to sharing of medicines information a point to bear in mind is that it this is already shared through referral letters. The issue is about checking its currency. The 4th principle of the Data Protection Act is that information is accurate and up to date. The GMC Good Medical Practice Duties of a Doctor states that doctors must "work with colleagues in the ways that best serve patients' interests."
>
> **What about consent?**
>
> In this instance the sharing of prescribing information would be done under the implied consent which allowed the initial referral to be sent. It would simply be allowing the prescribing information contained in the referral to be updated at the time the patient is actually seen. The intention of the original referral (ie. to provide accurate prescribing information to the specialist service) is supported and enhanced by this proposal.
>
> **Who would be able to access the information?**

Only the limited number of named individuals with a legitimate role relating to medicines reconciliation would be enabled to do this, authorised by suitably qualified senior staff.

Where would the information come from?

Partly because there are major changes to GP IT systems underway, it is not currently feasible to go direct to the patient's GP practice IT system for the information. As an interim measure most Boards may therefore look to the Emergency Care Summary as the source to retrieve the current prescription. This would mean a change in the use of this service and would require the agreement of the data controllers (ie GP practices and Boards) from whose systems the data is extracted.

In the medium to long term, more Boards are expected to implement the technology to allow retrieval of specific agreed information from local GP systems via their hospital-based clinical portal.

How would it be restricted to just those patients actually being seen at outpatients or being admitted?

An individual patient would have to be registered on the secondary care IT system as being due for an outpatient appointment or admission. And it would be via a check on this electronic record that the update request would be sent. Open-ended patient searching would not be a permitted means of accessing GP information.

How would you restrict the information to just what's needed, such as medication and allergies?

This is certainly not about access to the full GP record. For medicines reconciliation the electronic update request would be for agreed prescribing and allergy/adverse reaction information.

How would checks be done to make sure the rules were being followed?

An audit trail record of accesses for each patient would be maintained - who looked at what, when and from which computer system. This is already in place in relation to unscheduled care accesses to ECS. The log is analysed regularly in line with procedures established to act upon what may appear to be inappropriate access. A specialist software product to enhance this process is now available to NHS Boards. Note that this type of audit is not possible with paper case notes or phone calls.

All staff are required to keep up to date with and follow the laws and codes of practice that apply to their role. Staff are accountable for their actions when privacy or security breaches occur.

What would happen to staff who were found to have abused their responsibilities?

All staff are accountable for their actions to their employer and their profession for privacy or security breaches. Investigation of alleged incidents may result in disciplinary action in line with the Board's policies and procedures.

[Yours etc]

Annexe 1

Intra NHS Information Sharing

For NHSScotland organisations involved in the provision of Health Care Services for the people of Scotland

Further information is available at: www.ehealth.scot.nhs.uk

With acknowledgment to: NHS Wales Informatics Service

Contents

Introduction

The complexity of healthcare delivery in today's NHS means that there is a need to facilitate appropriate access to patients' information to ensure patients receive seamless health care as they move between primary and secondary care.

In addition, there is increasing emphasis on team working and considerable development in multidisciplinary delivery and management of care. It is therefore essential that healthcare professionals are able to communicate and share information in order to provide the best possible care for patients.

The provision of high quality, evidence based patient care requires the right information to be available to the right person at the right time. This means that patient information needs to be shared within and between NHS organisations[3] such as NHS Boards and GP Practices.

Within the NHS patient confidentiality is protected by common law and each individual employee's professional and contractual duties of confidentiality. Also the European Convention on Human Rights and the Data protection Act 1998 set the framework within which the privacy rights in relation to the processing of patient information are safeguarded.

All NHS organisations have Information Governance processes in place and have identified Caldicott Guardians who oversee access to, the use of and sharing of patient identifiable data with bodies both within, and outside NHSS[4]. The Patient Rights (Scotland) Act 2011 sets out the health care principles, including a commitment to respect an individual's privacy and confidentialty. The Act places a duty on NHS Boards to uphold the health care principles, and to ensure that those with whom they enter into contracts, agreements or arrangements uphold these principles when delivering healthcare.

1. Scope and Purpose

This document has been developed to facilitate the legitimate and justifiable sharing of personal identifiable information between NHS organisations for medical purposes[5]. The Data protection Act 1998 does not prohibit the collection and sharing of personal data – it provides a framework where personal information can be used in the confidence that individuals' privacy rights are respected.

This document applies to the exchange of information between:

- NHS Boards
- General Practitioners; and
- NHSScotland Administration Bodies e.g. NHS Healthcare Improvement Scotland, NHS National Services Scotland.

It also applies to 'cross border' information sharing between NHSScotland organisations and NHS organisations elsewhere in the UK.

[3] NHS Organisation: defined as Controllers under the Data Protection Act, either alone or jointly or in common determines the purpose for which and the manner in which personal data are, or are to be, processed

[4] Knowledge Network – NHSScotland Caldicott Guardians Website

[5] "medical purposes" includes preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

2. Consent

To comply with the Data Protection Act 1998 (and the Human Rights Act 1998), consent of the data subject is not a necessary precondition for lawful data sharing. The Data Protection Act 1998 sets out a number of criteria under Schedule 2 for the legitimate processing of personal data and more stringent criteria in Schedule 3 for Sensitive Personal Data and if any one of the criteria is met, the Data Protection Act 1998 test is satisfied. **Consent is an important but not an absolute criteria.** For the purposes of this document, there are two areas where explicit consent is not required as there are other conditions in Schedules 2[6] and 3[7] of the Data Protection Act that can be relied upon.

Common Law Duty of Confidentiality
If the patient has been informed what information is to be disclosed, the purpose and the extent of the disclosure, and that they have the right to object but have not objected then this is sufficient and explicit consent is not required for the following purposes:

1. Where patient information is used for the routine clinical care of that patient for example between health professionals and intra NHS multidisciplinary teams[8]

2. Where patient information is used for administration and management purposes, for example, waiting list management[9].

In addition, there are two other broad categories of information relating to individuals that NHS organisations may share without the need of an Information Sharing Protocol (ISP)[10] and these are as follows:

Aggregated (Statistical) Information
Aggregated and management information is used to plan and monitor progress of the organisation in its delivery of services. This is generally outside the scope of the Data Protection Act 1998 on the basis that a living individual could not be identified from such data.

Anonymised and Coded Information[11]
Information is said to be anonymised when the individual cannot be reasonably identified by the person or organisation to whom the information is being disclosed. Coded information may also be known as pseudonymised information. This is information from which individuals cannot be identified by those who receive the information, but which enables information about different patients to be distinguished. It also allows for information about the same patients to be linked over time such as to identify trends for example drug side effects. While this type of information would normally fall outside the scope of the Data Protection Act 1998, care must be taken with all coded and anonymised information as it may still be possible to identify individuals, e.g. with rare diseases, drug treatments or statistical analyses within a small population.

[6] Data Protection Act 1998 Schedule 2
[7] Data Protection Act 1998 Schedule 3
[8] Others who may be part of the healthcare team, but with whom patients might not expect information to be shared, include prescribing advisers who review patients' medicine needs to improve safety, efficacy and efficiency in doctors' prescribing.
[9] Use and Disclosure of Health Data - Information Commissioners Office May 2002
[10] An ISP details the purposes underlying the sharing of specific sets of information and communicates to Practitioners the operational requirements, setting out the who, what, why, where, when, and how of sharing information.
[11] Confidentiality: General Medical Council: London 2009

3. What does this mean for NHS organisations?

NHS organisations do not require explicit consent to share information between NHS professionals for medical purposes and there is **no** requirement to develop ISPs (Information Sharing Protocols) between NHS organisations.

Even though explicit consent will not be relied upon for the purposes identified in Section 2, each organisation must ensure that DPA 'fair processing' obligations[12] are met. This means that each NHS organisation should make sure information is readily available to patients explaining:

- Who holds their information;
- How their information may be used;
- With whom it will be shared; and
- The choices they have (except where sharing is required by law or are necessary for the provision of an essential service).

Patients must be made aware that their information may be used not only to provide them with care, but to support clinical or other service audit or work to monitor the quality of care/service provided. Patients can be given information in a range of ways including leaflets, talking with them etc, ensuring that language or other accessibility requirements are met appropriately.[13]

Patients must also be informed about other uses which inform the delivery and improvement of health and care services, support public health and provide benefits to society, e.g. health surveillance, disease registries and medical research.

Should a patient choose to refuse or limit the use of his / her information, the implications of such limitation or refusal must be clearly explained and the discussion clearly recorded in his / her health record.

Once information is sent in a referral letter (or copied from another system e.g. ECS) to an NHS organisation, the data is then controlled by that organisation who is then responsible for "fair processing."

4. Responsibilities

Patient identifiable information must be shared on a strict need to know basis with only the minimum necessary being shared. However, this must include sufficient information to ensure safe care and treatment – missing or incomplete information could present a significant patient safety issue.

The majority of patients understand that information relating to them will be shared within the NHSS in order to provide them with care. In doing so they expect a number of safeguards to be in place.

Each NHS Board and GP Practice:

- is responsible for ensuring the appropriate and lawful sharing of patient information between them and other organisations;

[12] Privacy Notices Code of Practice- Information Commissioners Officer December 2010
[13] Health Rights Information Scotland (HRIS): HRIS is commissioned by the Scottish Government Health Directorates to produce national information for people of all ages that use the NHS in Scotland.

- must have policies and procedures in place to ensure the integrity, availability and confidentialty of information processed. These should support legitimate and justifiable flows of intra NHS sharing and not restrict them;

- must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and shared. It is acknowledged that organisations will vary in size and complexity and this will be reflected in any processes and levels of security put into place.

When developing new IT systems or applications that enable personal information sharing (or significantly altering the scope or type of data collected on existing systems) the impact on individual's privacy and security concerns needs to be considered at the outset[14].

Each NHS employee[15] involved in the holding, obtaining, recording, using and sharing of patient identifiable information has a personal responsibility for ensuring the confidentiality and security of such information. Staff are responsible for making themselves aware of the laws and regulations which affect the job they do and the place where they work. This includes adhering to the NHSScotland Code of Practice on Protecting Patient Confidentiality[16], professional codes of practice[17] and/or guidance, and their organisation's policies and procedures.

[14] ICO Privacy Impact Assessments

[15] Staff who work for or are under contract to NHSScotland, including students, volunteers, contractors and independent contractors.

[16] NHSScotland Code of Practice on Protecting Patient Confidentialty

[17] The Regulatory Bodies include: the General Medical Council, Nursing and Midwifery Council, the General Dental Council, General Pharmaceutical Council and the Health Professions Council

5. Glossary

Term	Definition
Identifiable Information	Information which relates to an individual, including their image or voice, which enables them to be uniquely identified from that information on its own or from that and / or other information which is in the possession of, or is likely to come into the possession of the NHS organisation[18].
Wider Medical Purposes	Examples of 'wider medical purposes' are: • Clinical audit, for example, the monitoring of a patient care pathway against known standards and benchmarks. • Processing for administrative purposes, for example, disclosure by a GP made in order to receive payment for treatment provided. • Administrative audit, which may include studies designed to improve the efficiency of an NHS organisation, for example, to support decisions about the allocation of resources or service redesign. • Statutory disclosures for disease notification • Disclosures to disease registries or disclosures for epidemiological research. Many specific flows of information have already had guidance and Regulations published in their support. Cancer Registries for example undertake a range of public health surveillance and health protection functions. These regulations make it both lawful and appropriate to share confidential patient information in the specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. Consent does not have to be obtained.
Consent	An informed indication by which the individual signifies his/her agreement and understanding of how personal identifiable data relating to them is to be processed.
Express Consent	Consent which is expressed orally or in writing. Also known as explicit consent[19].

Processing, in relation to information means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination[20]

[18] Data Protection Act 1998: Part 1 Section 1 (1)
[19] Confidentiality: General Medical Council: London 2009
[20] Data Protection Act 1998: Part 1 Section 1 (1)