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

V1 Published Dec 2011
KKingan, eHealth
INTRODUCTION

1. 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.

2. 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.

3. 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 such as NHS Boards and GP Practices.

4. 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.

5. 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. The Patient Rights (Scotland) Act 2011 sets out the health care principles, including a commitment to respect an individual’s privacy and confidentiality. 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.

SCOPE AND PURPOSE

6. This document has been developed to facilitate the legitimate and justifiable sharing of personal identifiable information between NHS organisations for medical purposes. 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.

7. 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.

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

---

1 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

2 Knowledge Network – NHSScotland Caldicott Guardians Website

3 “Medical purposes” includes preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
CONSENT

9. To comply with the Data Protection Act 1998 (and the Human Rights Act 1998), consent of a data subject is not always 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. 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 when other conditions specified in Schedules 2\(^4\) and 3\(^5\) of the Data Protection Act can be relied upon.

COMMON LAW DUTY OF CONFIDENTIALITY

10. 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:

- Where patient information is used for the routine clinical care of that patient - for example between health professionals and intra NHS multidisciplinary teams\(^6\)
- Where patient information is used for administration and management purposes, for example, waiting list management\(^7\).

11. 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)\(^8\) and these are as follows:

AGGREGATED (STATISTICAL) INFORMATION

12. 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\(^9\)

13. Information is said to be anonymised when the individual cannot be reasonably identified by the person or organisation to which 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

\(^4\) Data Protection Act 1998 Schedule 2
\(^5\) Data Protection Act 1998 Schedule 3
\(^6\) 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.
\(^7\) Use and Disclosure of Health Data - Information Commissioners Office May 2002
\(^8\) 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.
\(^9\) Confidentiality: General Medical Council: London 2009
information as it may still be possible to identify individuals, e.g. with rare diseases, drug treatments or statistical analyses within a small population.

WHAT DOES THIS MEAN FOR NHS ORGANISATIONS?

14. 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.

15. 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\textsuperscript{*10} 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).

16. 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.\textsuperscript{*11}

17. 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.

18. 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.

19. 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.”

RESPONSIBILITIES

20. 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.

21. 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.

\textsuperscript{*10} Privacy Notices Code of Practice- Information Commissioners Officer December 2010

\textsuperscript{*11} 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.
22. Each NHS Board and GP Practice:

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

- Must have policies and procedures in place to ensure the integrity, availability and confidentiality 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.

23. 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 by undertaking a privacy impact assessment\textsuperscript{12}.

24. Each NHS employee\textsuperscript{13} 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\textsuperscript{14}, professional codes of practice\textsuperscript{15}, the Caldicott Principles and/or guidance, and their organisation’s policies and procedures.

\textsuperscript{12} ICO Privacy Impact Assessments

\textsuperscript{13} Staff who work for or are under contract to NHSScotland, including students, volunteers, contractors and independent contractors.

\textsuperscript{14} NHSScotland Code of Practice on Protecting Patient Confidentiality

\textsuperscript{15} The Regulatory Bodies include: the General Medical Council, Nursing and Midwifery Council, the General Dental Council, General Pharmaceutical Council and the Health Professions Council
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifiable Information</td>
<td>Information that 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(^16).</td>
</tr>
<tr>
<td>Wider Medical Purposes</td>
<td>Examples of ‘wider medical purposes’ are:</td>
</tr>
<tr>
<td></td>
<td>• Clinical audit, for example, the monitoring of a patient care pathway against known standards and benchmarks.</td>
</tr>
<tr>
<td></td>
<td>• Processing for administrative purposes, for example, disclosure by a GP made in order to receive payment for treatment provided.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Statutory disclosures for disease notification</td>
</tr>
<tr>
<td></td>
<td>• Disclosures to disease registries or disclosures for epidemiological research.</td>
</tr>
<tr>
<td>Consent</td>
<td>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.</td>
</tr>
<tr>
<td>Express Consent</td>
<td>Consent which is expressed orally or in writing. Also known as explicit consent(^17).</td>
</tr>
<tr>
<td>Processing</td>
<td>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(^18)</td>
</tr>
</tbody>
</table>

\(^{16}\) Data Protection Act 1998: Part 1 Section 1 (1)  
\(^{17}\) Confidentiality: General Medical Council: London 2009  
\(^{18}\) Data Protection Act 1998: Part 1 Section 1 (1)