

Data Sharing Review Secretariat,
5.26 Steel House,
11, Tothill Street,
London SW1H 9LH

Dear Sirs,

Data Sharing Review: A consultation paper on the use and sharing of personal information in the public and private sectors

The UK Council of Caldicott Guardians (UKCGC) is an elected body made up of Caldicott Guardians from across the UK representing NHS, Independent health sector and Social Care organisations in England, Wales, Scotland and Ireland. It was created in 2005 to:

- be the UK national body for Caldicott Guardians;
- promote the roles and activities of Caldicott Guardians;
- be a forum for the exchange of information, views and experience;
- represent the views of Caldicott Guardians on matters of policy relating to Information Governance;
- be a channel of communication with national organisations concerned with the NHS, the independent health sector, local government and health and social care professionals; and
- be a resource centre, to provide support and arrange learning opportunities for Caldicott Guardians

The Council consists of 19 registered Caldicott Guardians from all of the Home Countries representing health and social care organisations, with lay representation from the Patient Information Advisory Group - an advisory body to the Secretary of State for Health set up under s.60 of the Health and Social Care Act 2000.

It was the debate generated by many, including especially the BMA, over the announcement of the electronic health record in the mid 1990s that led the then government in 1997 to ask Dame Fiona Caldicott to review patient-identifiable information in the NHS. Her Report, in December 1997, identified weaknesses in the way parts of the NHS handled confidential patient data. The Report made a number of recommendations for regulating the use and transfer of Patient-Identifiable information between NHS organisations in England and to non-NHS bodies. That last clause is important – the recommendations cover data sharing within the NHS and with non-NHS bodies. By extension, the recommendations have been applied to the independent sector both in its dealings with the NHS and generally.

The Report also recommended the appointment of Caldicott Guardians - a Senior Person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

The Caldicott Committee's remit included all patient-identifiable information passing between organisations for purposes other than direct care, medical research or, where there was a statutory requirement for information. The aim was to ensure that patient-identifiable information was shared only for justified purposes and that only the minimum necessary information was shared in each case. The Committee also advised on where action to minimise risks of confidentiality would be desirable.

Caldicott Guardians were introduced into the NHS from 1 April 1999 as a result of the recommendations of the Caldicott Committee, and were subsequently introduced into Social Care in 2002. They were mandated by Ministers through a Health Service Circular and have

since become firmly established as part of the infrastructure of Information Governance and protecting the confidentiality of Health and Social Care Data.

The role of Caldicott Guardians has evolved since their introduction and continues to evolve as the NHS seeks to retain public confidence in the new IT systems and to reassure those who are concerned that the confidentiality measures are robust.

We have commented only on those questions where we believe we have a direct interest.

Question 1: Please explain what your interest in information sharing is.

The Caldicott Guardian should play a key role in ensuring that NHS, local authorities, voluntary and independent sector organisations satisfy the highest practical standards for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. Acting as the ‘conscience’ of an organisation, the Caldicott Guardian should also actively support work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required. Local issues will inevitably arise for Caldicott Guardians to resolve. Many of these will relate to the legal and ethical decisions required to ensure appropriate information sharing. It is essential in these circumstances for Guardians to know when and where to seek advice.

A key recommendation of the Caldicott Committee was that every use or flow of patient-identifiable information should be regularly justified and routinely tested against the principles developed in the Caldicott Report.

The Caldicott Guardian Principles, the Data Protection Act and the Freedom of Information Acts are all linked:

- the Data Protection Act is about equality, fairness and privacy in the way information is processed;
- the Caldicott Principles are about Privacy and Confidentiality in sharing information; and
- Freedom of Information is about public’s right to know how these are regulated within public organisations - policies, procedures and Information Sharing Protocols.

There is a high correlation between the Caldicott Principles and the Data Protection Act Principles as can be seen from the table below.

The Caldicott Principles	The Data Protection Principles
1 - Justify the purpose(s) for using confidential information	3, 6
2 - Only use it when absolutely necessary	3, 6
3 - Use the minimum that is required	3
4 - Access should be on a strict need-to-know basis	3, 6, 7
5 - Everyone must understand his or her responsibilities	7
6 - Understand and comply with the law	1,2

Medical and social care confidentiality has never been absolute but has operated on a principle of limiting disclosure to those who need to know, giving them only and as much information as they need. This general rule is waived where, for example, a breach of confidence is required by law or where the individual gives valid consent. In addition to statute protection of confidentiality there is the common law duty of confidentiality.

There has been disclosure of patient identifiable data between the NHS and the independent sector since the inception of the NHS. Strictly speaking, GPs are independent practitioners contracted to provide medical services to the NHS – the *Data Controller* for a patient's GP record is the Secretary of State for Health.

The whole area of health and social care is a complex one with many Agencies involved in both routine and ad hoc interactions. This complexity has been further complicated by the split of Social Care split between Adult and Children, often reporting to different parts of the Local Authority.

Data sharing is a complex and emotive subject. There is often confusion about disclosure to, or sharing with, third parties. There is a significant difference in law between disclosure to an Independent Provider who is acting as a *Data Processor* for the Trust and disclosure to a third party where that third party is a *Data Controller*. There are many circumstances where there is disclosure to a third party with informed patient consent: NHS GP to private consultant and vice versa; NHS A&E Department to the Samaritans or other Voluntary Sector organisation, especially over a week-end; or a tertiary referral to a specialist private consultant. Most of these examples are with oral consent.

The above examples are all to do with health care or support provision. There are other agencies who may also have a legitimate requirement for access to a sub-set of the health record, e.g. Education and Social Care. Whatever the reason it ought to be transparent and in accord with the Fair Obtaining Notice and the requirements of the Data Protection Act and any other regulations and legislation. Access to files containing medical or other confidential information should, of course, be limited to individuals who have a proper reason for needing it. Once a file has been accessed, it should be read only for what is relevant to the job in hand – easier to implement in an electronic environment.

Data held within NHS systems contain health data and non-medical personal data, e.g. demographic data; expenses etc. Data held in the Secondary Uses System (SUS) contains both named data and anonymised data. It is important to differentiate between sharing named data and anonymised data.

There may also be circumstances in which an individual's health data should be disclosed in the public interest, i.e. for public health and disease monitoring purposes. Such cases will need a careful balancing of the right to confidentiality of the individual and the needs of society.

There will be other cases such as the Police, NHS Counter Fraud, GMC where there are statute obligations for disclosure.

Question 9: In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

Some Council members thought the Act was too restrictive and was damaging British research interests, whilst others thought it was vague and inflexible, and created problems for those trying to apply it.

One member felt that the Act's interaction with the NHS Code of Confidentiality was unhelpful and that legalistic concepts of consent should be opposed. There should be a distinction made between the different secondary uses, i.e. those where information is being transferred

for use as identifiable personal data, and those where information is transferred and then anonymised, e.g. disease registries.

It was felt that the Act should have more useful content regarding the handling of third party data obtained whilst dealing with the first party.

Question 20: What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.

Council considered that technological advances do provide significant benefits for patients and service users:

- access to an individual's records when the caring professional needs access and at the location of service delivery;
- the ability to enforce role based access to all or part of a record; and
- to provide accountability through logging of all accesses.

They also noted that there are downsides with the technological advances: Paper records can only be stolen by one person at a time, whereas electronic records may be stolen or disclosed in much larger numbers, on more than a single occasion and by more people, as has been so amply demonstrated over recent months.

Question 27: Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering?

Patients and service users entrust health and social care providers, or allow them to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients and service users is to be retained, that the health and social care providers provide, and are seen to provide, a confidential service. The Independent and voluntary sectors are subject to the same professional codes, legislation, common law and regulation. It should be noted that these expectations of confidentiality pre-dated the Data Protection Acts.

There needs to be advice about information sharing protocols, i.e. whether they are useful, what they can do, what they can not do etc. and how to incorporate them into daily working practices. An opinion was expressed that such protocols are actually a distraction from good working practices. Particularly as similar organisation types often work in very different ways. It was pointed out that in social services there were internal boundaries that had to be addressed e.g. adult social care and housing are often in the same department now. This requires that operational staff are informed of what they can and cannot do with personal information; not a high level protocol about what will be shared with external organisations.

Question 28: Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

The Council believes that once all the responses have been received consideration should be given to setting up an expert working group with public representation to develop guidance.

Information governance is a system of policies and procedures, standards and guidelines which establish a framework for defining who is responsible for what and how decisions are made. It puts in place mechanisms for ensuring that systems work the way they were meant to. It is a complex interplay between law, ethics and policy.

The Healthcare Commission has made Information Governance a core standard for every health care organisation to have information governance in place, expressed as: Confidentiality: the duty to protect; Security: the accuracy of data and access; and Privacy: the right not to be known

The most visible manifestation of Information Governance within the NHS and Social Care has been the Information Governance Toolkit. Within NHS Connecting *for* Health Information Governance is defined as *“the structures, policies and practice of the healthcare industry, the DH, the NHS, the Independent sector and its suppliers to ensure the confidentiality and security of all records, and especially patient records, and to enable the ethical use of them for the benefit of individual patients and the public good”*.

Essentially, the IG Toolkit has been developed from the ISMS (Information Security Management System) Code of Practice ISO/IEC 27002 (formerly known as ISO/IEC 17799, formerly BS7799 Part 1). The IG Toolkit consists of IS security standards and management processes which are scored and evidenced. The toolkit has to be completed annually and a return submitted to the Digital Information Policy Group at Connecting *for* Health and the National Information Governance Board for Health and Social Care. Any Independent provider or commissioner who require connectivity to the NHS Net also have to complete an annual IG Toolkit and reach a minimum standard to obtain and retain connectivity. In addition, Independent providers or commissioners must also be certified to ISO/IEC 27001 (formerly known as BS7799 Part 2) as a condition of connectivity.

The Council strongly believes that the Information Governance Standards should be applied to all government departments.

**Chairman, UK Council of Caldicott Guardians
Group Information Protection Manager & Caldicott Guardian, BUPA**