

Developments in confidentiality and consent functions to support wider sharing of electronic health records in the UK

With increased pressure for enhanced medical record availability comes concerns about privacy and consent. **Stephen Elgar** and **Shane Balfe** consider how consent functions have been developed to support the sharing of records within England.



HOME

THE
EXPECTATION
OF PRIVACY

THE ROLE
OF PATIENT
CONSENT IN
SHARING
MEDICAL
RECORDS
WITHIN THE UK

THE CONSENT
MODEL FOR
THE SUMMARY
CARE RECORD

CONCLUSIONS

summary

Healthcare has particular requirements for privacy and consent when it comes to the sharing of medical records. Current practice dictates that a patient's medical record is collected and held within the organisation that is providing care. However, there is increased pressure from many stakeholders for enhanced record availability from different care providers and using different technologies for accessing medical records. In this article, we consider how consent functions have been developed to support the sharing of records within England, the largest of the four Home Countries of the UK.

In today's world, individuals increasingly expect service providers to have information continuously available, in convenient formats and via different media. For an industry such as banking, customers expect their account information to be readily accessible through physical visits to any bank branch and via remote access through phone-based banking services or through Internet channels. This level of service expectation provides challenges for the healthcare industry where traditionally the primary care giver will maintain medical records locally.

As many patients will move a number of times within their lifetime, a patient's medical records can become fragmented following episodes of care in a sequence of different providers. The Summary Care Record (SCR) in England was

developed to improve availability of information for emergency care. The SCR contains information such as active medication, allergies, contra-indications and documents such as discharge summaries, and is drawn from the patient's long-term record held by their General Practice teams. At the time of writing, the SCR is available for almost 10% of the population within the United Kingdom. Given the sensitivity of this record, the prevention of its unauthorised use is of obvious concern to the patient and, for NHS care-providers, gaining access to this record rests on gaining the patient's consent.

Electronic health records have become essential tools for the support of medical care. At one time, access to these records was limited to just the organisation providing primary care to the

[HOME](#)[THE EXPECTATION OF PRIVACY](#)[THE ROLE OF PATIENT CONSENT IN SHARING MEDICAL RECORDS WITHIN THE UK](#)[THE CONSENT MODEL FOR THE SUMMARY CARE RECORD](#)[CONCLUSIONS](#)

patient. However, to support citizens’ ability to move home multiple times within their lifetime, to travel for work and leisure, or where a medical condition requires tests, has complications or becomes persistent, there is an increasing need to extend the availability of medical record information beyond their primary carer. This extended access presents many difficult security challenges in maintaining patient privacy.

THE EXPECTATION OF PRIVACY

When one goes to the doctor, there is an expecta-

tion that your discussion and any diagnosis and treatment information will be kept private. Should this expectation not be respected, a patient might withhold information the next time they visit or perhaps withdraw from treatment altogether. For the doctor, this expectation of privacy and trust is at the core of the relationship with the patient. This is reflected in part of the doctor’s commitment to the statement of professional ethics, the 6th century BC Hippocratic Oath: — “All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret

FIGURE 1

NUMBER OF NHS STAFF AND ORGANISATIONS IN ENGLAND

<p>10,000 GP Practices*</p> <p>360 Hospitals</p> <p>100 Community orgs.*</p> <p>100 Mental Health orgs.*</p> <p>500 Voluntary orgs.*</p> <p>50 Private health providers into the NHS*</p> <p><i>* indicative figure</i></p>	<p>1.3 M Staff</p> <p>35k GPs</p> <p>32k Consultants</p> <p>400k Nurses</p> <p>134k Paramedics</p> <p>360k Admin. support staff</p>	<p>106 M Patient records</p> <p>51M Patients registered with GPs</p> <p>15M Hospital inpatient episodes (annual)</p> <p>30M Hospital outpatient episodes (annual)</p> <p>12M First A&E attendance</p>
---	--	--

HOME

THE EXPECTATION OF PRIVACY

THE ROLE OF PATIENT CONSENT IN SHARING MEDICAL RECORDS WITHIN THE UK

THE CONSENT MODEL FOR THE SUMMARY CARE RECORD

CONCLUSIONS

and will never reveal.”

However, the reality of modern healthcare is not based exclusively on a private understanding between a patient and a doctor. Modern healthcare is organised in specialist teams with paramedic and support staff spread across many organisations. In England there is a direct healthcare workforce of over 1.3 million (out of a population of some 51 million) in 11,000 separate organisations — see in [Fig. 1](#). The task of establishing appropriate identification, authentication and access control for this workforce to cater for shared access to medical records is considerable.

Since 2003, there has been a £12 billion investment in a new National Care Record Service (NCRS) in England. The NCRS provides a national patient index with demographic details and patient services, such as the Choose and Book service for referral to hospital and the Electronic Prescription Service to send a GP script directly to a high street pharmacy. In many NHS organisations, the NCRS is additionally used to access patient medical record systems. The English Summary Care Record (SCR) is part of NCRS and makes use of the NCRS security services and functions to maintain confidentiality and enable access on the basis of patient consent.

THE ROLE OF PATIENT CONSENT IN SHARING MEDICAL RECORDS WITHIN THE UK

The security policy for sharing medical records results from the interplay of individual rights, professional practice and organisational obligations. It is based on a complex legal framework which includes Common Law Duties of Care and Confidentiality, the Human Rights and Data Protection Acts, the Computer Misuse Act and a series of specific health related Acts and regulations. For example, Common Law stipulates a duty of confidentiality for all parties in the provision of healthcare services. Similarly, the Data Protection Act (1998) provides rights for individuals with informed consent as the basis for any sharing of information. Thus, the legal basis for sharing medical records is founded upon the necessity of gaining patient consent. Within the NHS, there are two models of consent that are used by health care providers for gaining access to patient health care records: implicit and explicit consent.

IMPLIED CONSENT

Patients are made aware of the purpose and use of their information through posters and leaflets on display throughout the NHS. These “fair processing” notices are intended to establish an

HOME

THE
EXPECTATION
OF PRIVACY

THE ROLE
OF PATIENT
CONSENT IN
SHARING
MEDICAL
RECORDS
WITHIN THE UK

THE CONSENT
MODEL FOR
THE SUMMARY
CARE RECORD

CONCLUSIONS

TABLE 1

ENGLISH NHS BEST PRACTICE GUIDE FOR CONSENT OBLIGATIONS FOR HEALTHCARE ORGANISATIONS 2009 [<http://www.nigb.nhs.uk/guarantee>]

- Allow patient to control whether the information recorded about them by an organisation providing them with NHS care can be seen by other organisations that are also providing them with care;
- Show only those parts of patient record needed for patient care;
- Allow only authorised people to access patient record;
- Allow only those involved in patient care to have access to records about them from which the patient can be identified, unless the patient gives permission or the law allows;
- Allows use of information about patient health-care, in a way that doesn't make patient identity known, to improve the services offered or to support research;
- Keep a note of everyone who accesses a patient's records; and be operated in line with internationally approved information security standards.

informed basis for creating, maintaining and sharing a medical record. However, many patients will not read these notices. For a patient, a more pressing concern is often to understand their condition, the treatments available and whether or not to proceed. Similarly, for the clinician, the urgency of gaining consent for treatment will trump other consent aspects. Perhaps as a response to this, there is an assumption that patients reasonably expect information sharing by staff involved in their care. To be asked for permission on each occasion that their record is accessed would be impractical and undesirable, so a practice of tacit consent for sharing within a given care team is followed. This practice extends along the pathway of care and its associated processes for investigation and treatment, a path of which the patient is unlikely, and would probably not want, to be aware. This practice of implied consent has become established as a compromise with the legal principle of active or explicit consent.

EXPLICIT CONSENT

As a limit to sharing medical records, the organisational boundary is identified as a significant point of control and it is here that explicit control

HOME

THE
EXPECTATION
OF PRIVACYTHE ROLE
OF PATIENT
CONSENT IN
SHARING
MEDICAL
RECORDS
WITHIN THE UKTHE CONSENT
MODEL FOR
THE SUMMARY
CARE RECORD

CONCLUSIONS

mechanisms are placed. [Table 1](#) lists considerations for implied consent for sharing medical records within NHS organisations.

IT systems must have an access control model with appropriate authorisation to ensure the minimisation of user access, appropriate to their role and relationship to the patient. Any access that is not related to direct patient care must be restricted to anonymised data. Audit facilities must allow a listing of who has seen what. Explicit patient consent has to be recorded for exchange at the boundary. A range of confidentiality functions illustrated in [Table 1](#) has been implemented within the NCRS to meet these obligations.

To satisfy legal requirements, patients must be informed about how their medical record is produced, maintained and used, and given choice as to how their health information is shared. NHS policy fulfils this requirement using the principle of implicit consent along the pathway of care and the need for explicit consent controls, where possible, for exchange at the organisation boundary. This is a compromise which enables the accountability of individual staff and their employing organisation while still giving the record freedom of movement within an organisation and exchange at its boundary.

Are there exceptions to patient privacy and

consent requirements?

For the good of its citizens, privacy for the medical record has to be balanced against accessibility. For example, when a patient is unconscious and severely injured, the clinician has a duty of care, which, at the point of crisis, overrides patient privacy. If your loved one has been knocked down in the street, there is an expectation that everything possible would be done to keep them alive and make them better. Once they have recovered, privacy and consent issues re-emerge, but for the episode of emergency care these will typically need to be temporarily put aside.

Other examples of exceptions to patient privacy concerns relate to health risks to the public. For example, in a consultation, if a psychiatrist becomes convinced that there is a significant threat of violence, then they are obliged to alert the police. In other settings, clinicians are obliged to report diseases such as tuberculosis and HIV to public health authorities to allow the tracking and management of the disease and/or to assess long-term epidemiological patterns of diseases. In such situations, the patient may not be aware of the sharing of their medical record with other parties. The reason for sharing must be recorded in the patient record and the clinician and their employing organisations can, of

HOME

THE
EXPECTATION
OF PRIVACY

THE ROLE
OF PATIENT
CONSENT IN
SHARING
MEDICAL
RECORDS
WITHIN THE UK

THE CONSENT
MODEL FOR
THE SUMMARY
CARE RECORD

CONCLUSIONS

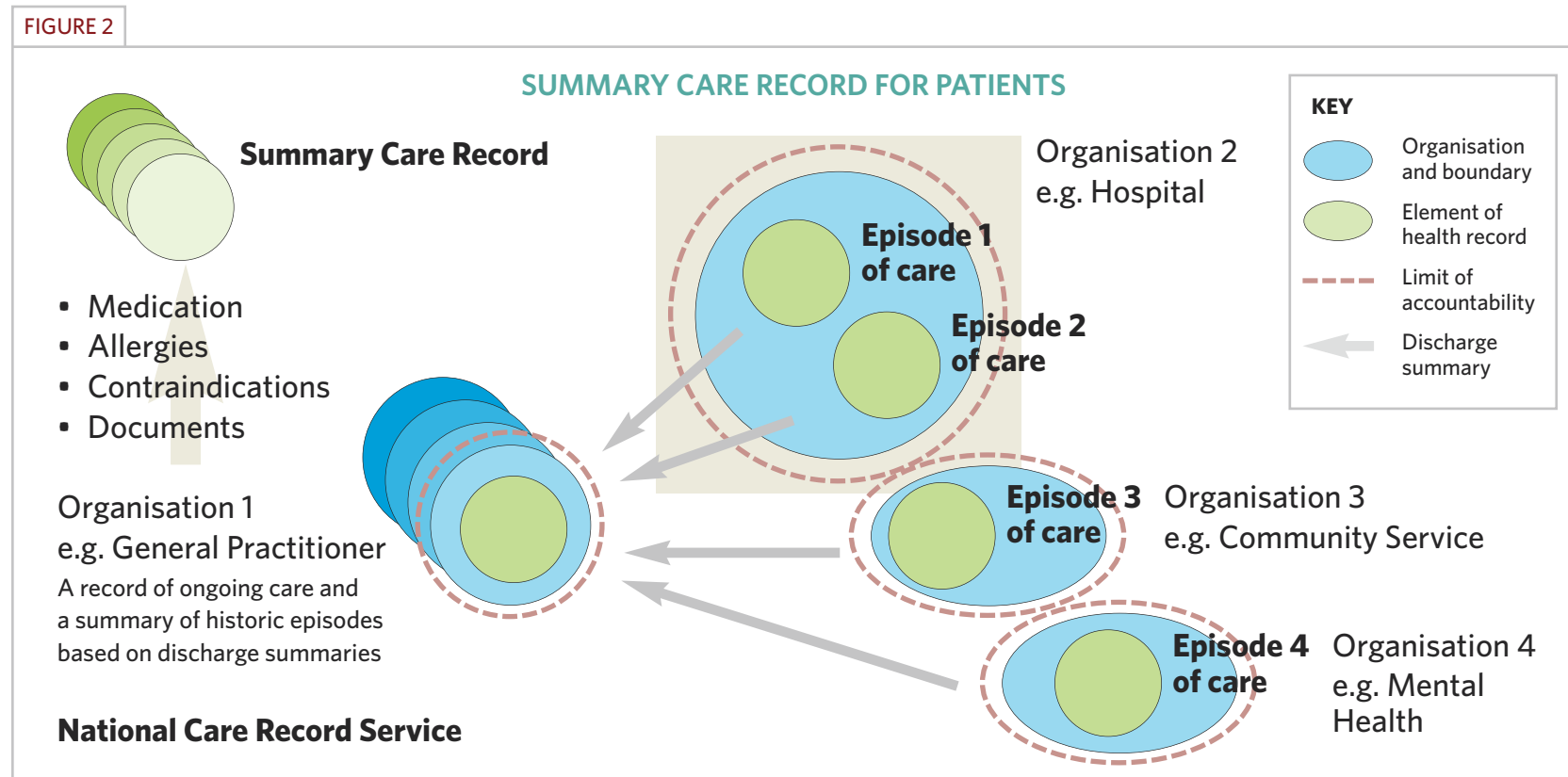
course, be held to account.

In contrast, services such as sexual and reproductive health provision are provided on the basis of anonymity. A more challenging element of a consistent NHS privacy policy concerns patients who undergo gender reassignment. Criminal action can be taken if reference is made to their former selves and special arrangements are required to manage the common NHS index for

these patients. A discussion of the practical implications of this complex policy is available from the General Medical Council.

THE CONSENT MODEL FOR THE SUMMARY CARE RECORD

As we have seen, privacy of medical data can be a complex arrangement between tacit and explicit



HOME

THE EXPECTATION OF PRIVACY

THE ROLE OF PATIENT CONSENT IN SHARING MEDICAL RECORDS WITHIN THE UK

THE CONSENT MODEL FOR THE SUMMARY CARE RECORD

CONCLUSIONS

consent. The introduction of the SCR is intended to simplify this process by providing access to a limited and controlled part of the medical record for emergency purposes (which is taken from the GP long-term record). The SCR contains active medications, allergies, contra-indications and, potentially, documents such as discharge summaries and care plans.

This minimal content of the SCR and its direct control by the GP reduces patient consent issues. [Figure 2](#) illustrates the problem space by way of example, describing how the SCR record can be linked to medical records in a number of health-care providers. Common record identification is maintained by the NCRS, which supports a shared NHS number and demographic details. Each of the four organisations in the diagram has a separate medical record for each episode of care for the patient. Release of this record is under the control of each host clinical team within each organisation. It can only be passed to another clinical team if access is necessary for care of the patient.

When the GP team orders a service or a referral, an automated request is sent to the provider, and results and summaries returned to the GP. This exchange is on the basis of implicit consent following the patient seeking care from the GP

team. On the other hand, explicit consent of the patient is required for an SCR record because this element of the medical record will be available outside the GP practice wherever and whenever it is needed rather than as part of a planned episode of care.

Management of the SCR by the GP team reflects the model of UK healthcare where the GP has a personal knowledge of the patient, his family and the community.

Management of the SCR by the GP team reflects the model of UK healthcare where the GP has a personal knowledge of the patient, his family and the community. The GP is a gatekeeper to hospital and other services, and a custodian of a long-term record for the patient. A similar arrangement exists for another voluntary element of the medical record, the living will, a note of the patient's wishes for extreme circumstances such as coma and vegetative state.

HOME

THE
EXPECTATION
OF PRIVACY

THE ROLE
OF PATIENT
CONSENT IN
SHARING
MEDICAL
RECORDS
WITHIN THE UK

THE CONSENT
MODEL FOR
THE SUMMARY
CARE RECORD

CONCLUSIONS

For the launch of the English SCR, a letter was sent to each household explaining the development and offering an “opt out” mechanism through the GP team. So far 0.1% of patients have chosen not to have an SCR record. There are many reasons why a patient may not wish to have such a record. One concern could be the ease of inference from medications such as anti-depressants (mental illness), contraceptives (sexually active) and more exotic drugs such as chemical castration (paedophile).

A second consent control exists for the SCR. At the point of care, the emergency team asks “permission to view” the record. This control was added after an initial pilot concluded that patients were confused by the nature of an SCR, the choices available and could change their mind at any time.

The SCR is about to enter into mass usage across English NHS for Accident and Emergency departments, and out of hours and palliative care teams, as records are progressively added by GPs. A secure network links all NHS organisations with “rules of the road” based on the ISO/IEC 27002 standard. Use of this standard is maturing and organisations are now required to conduct an annual audit and publish a compliance statement. This shared commitment provides a consistent level of security for the SCR.

At present, most access is from fixed locations but mobile channels are available and there are plans to use them in ambulances.

CONCLUSIONS

The SCR development in England should be seen as a simple way of providing wider access to the medical record. Confidentiality is based upon a shared approach to security across organisations and upon specific controls and functions present within the system. NCRS consent mechanisms provide a log of patient decisions for purposes of legal compliance. The low rate of opt-out can support a view that the vast majority of patients do not have privacy concerns and it is often said that patients believe this information is already widely available.

Content of SCR could be easily extended to include more of the GP record. The SCR could also provide content for Personal Health Records (PHR), a new type of the medical record directly controlled and held by the patient (see Google Health and Microsoft HealthVault). The advantage of the SCR as a source for a PHR is that its NHS integrity and provenance is known and, through NCRS services, could be digitally signed. ■

HOME

THE
EXPECTATION
OF PRIVACY

THE ROLE
OF PATIENT
CONSENT IN
SHARING
MEDICAL
RECORDS
WITHIN THE UK

THE CONSENT
MODEL FOR
THE SUMMARY
CARE RECORD

CONCLUSIONS

ABOUT THE AUTHORS

Stephen Elgar took a degree in Geography, trained as a nurse and then worked for 15 years in IT within the NHS as Project Manager and then team leader. For the last eight years he has worked in London putting the Care Record Service, a £12 billion IT investment, into use as Information Governance and Security Manager for NHS London. His main focus has been on the confidentiality functions of patient applications including a Registration Authority in London with 90,000 smart-cards supporting authentication and digital signature. Other responsibilities include data quality, the NHS security compliance and supporting organisations in management of data loss incidents.

Shane Balfe is currently studying for a Ph.D. in Information Security at Royal Holloway. His main areas of research interest are in trusted computing and ad-hoc networks.

HOME

THE
EXPECTATION
OF PRIVACY

THE ROLE
OF PATIENT
CONSENT IN
SHARING
MEDICAL
RECORDS
WITHIN THE UK

THE CONSENT
MODEL FOR
THE SUMMARY
CARE RECORD

CONCLUSIONS