THE NPFIT STRATEGY FOR INFORMATION SECURITY OF CARE RECORD SERVICE

Yara Mohammad, Ministry of Health, Damascus, Syria, yara.mohammad@gmail.com

Lampros Stergioulas, School of Information Systems, Computing & Mathematics, Brunel University, UK, lampros.stergioulas@brunel.ac.uk

Abstract

The National Programme for IT in England doesn't have a one-document strategy for its information security of the Care Records Service, which is the national EHR system. This paper provides a comprehensive understanding of the information security strategy of England's EHR system by presenting its different information security issues such as consent mechanisms, access control, sharing level, and related legal and regulations documents.

Keywords: Electronic Health Records, Information Security, Strategy, NPfIT.

1 INTRODUCTION

Information security strategy of EHR systems is a roadmap for the foreseeable future that details the progress along the path of system maturity and keeps the focus on the most important security issues while complying with legal, statutory, contractual and internally developed requirements (Purser, 2004) for electronically stored and shared information to support continuing, efficient and quality integrated healthcare provided by different healthcare professionals (Hayrinen et. al, 2008).

It is essential to understand the existing information security strategy of any EHR system by bringing it all together into one document that is readable and approachable for monitoring and development by EHR users and developers.

There is no one written strategy document that clarifies how information will be secured during and after implementing shared electronic health records in the National Programme for Information Technology (NPfIT) in England. This paper focuses on providing an understanding of the NPfIT information security strategy.

Different information regarding information security in Electronic Health Records (EHR) in England was shared and published by the National Health Service (NHS) in England, and different visions and mechanisms were proposed to be in place when the NPfIT is being implemented. This paper presents

all captured information during this research that was given, published and presented by NHS Connecting for Health (CfH) professionals from different and various sources, in an attempt to understand the NPfIT strategy for information security of the Care Record Service (CRS) in England.

In this paper an overview of shared electronic health records in England will be presented. Then, the care record service (CRS) design will be discussed including different information security mechanisms such as NHS smartcard, National Network for the NHS (N3), access control, legitimate relationship, alerts, audit trails, sealed envelopes, and the consent model. Furthermore, this paper will present and discuss different relevant sets of documents that concern information security of electronic health records in the NPfIT which includes different standards and legal Acts.

2 RESEARCH METHODOLOGY

A major case study with ethnographic research method of the National Programme for IT (NPfIT) in England is carried out. To be able to collect data for this research, different research methods were applied. These methods are explained below:

2.1 Participant observation - Networking

An ethnographic method was used in this research by ongoing observation, both structured and unstructured (Crespin et al., 2005). "*In ethnography, these data sources are supplemented by data collected through participant observation. Ethnographies usually require the researcher to spend a long period of time in the "field" and emphasize detailed, observational evidence*" (Myers, 1999). The ethnographic research method was used by Orlikowski (1991) who collected his research data via participant observation, interviews, documents, and informal social contact with the participants (Myers, 1999).

Participation in Connecting for Health (CfH) events, along with sharing knowledge and providing ideas and suggestions in various NHS CfH workshops and conferences, helped identifying key issues and finding solutions. Attendance of these events also provided up-to-date information and data of the NHS Care Records Service (NCRS).

In addition, joining some NHS specific networks and being a member of them allowed sharing knowledge. This online community includes some NHS CfH Special Interest Groups which were organising regular meetings to discuss some specific issues related to health informatics in the NHS in general and to NHS Care Records Service (CRS) in particular. There were many opportunities in taking part in other NHS CfH forums and networking activities which organised regular meetings,

workshops and conferences to raise and discuss up-to-date issues related to the NHS Care Records Service in the London Cluster.

The researcher interviewed different NHS staff and software providers informally during the attended events. Notes were taken by the researcher in these events, in addition to the presentations and different documents were shared after attending the events.

2.2 Document analysis

Some documents were released by different organisations, such as Department of Health, NHS CfH, Ministry of Justice and International Organisation for Standardisation to define EHR systems deployment policies which are related to confidentiality and security concerns. These documents were analysed critically to show related parts that are important to protect the user's right for confidential and secure medical data.

3 AN OVERVIEW OF SHARED ELECTRONIC HEALTH RECORDS IN ENGLAND

The National Programme for Information Technology (NPfIT) in the National Health Service (NHS) in England is a ten year programme which presents an unprecedented opportunity to use Information Technology (IT) to reform the way the NHS in England uses information, and hence to improve services and the quality of patient care. The core of the programme is the NHS Care Records Service (CRS), which is planned to make relevant parts of patient's clinical record available to whoever needs it to care for the patient. The programme also includes many other elements, including X-ray accessibility by computer, electronic transmission of prescriptions, and electronic booking of first outpatient appointments (NAO, 2006).

The NHS CRS is supposed to enable each person's detailed records to be securely shared between different parts of the local NHS, such as the GP surgery and hospital. Patients will also be able to have a summary of their important health information, known as their Summary Care Record available to authorised NHS staff treating them anywhere in the NHS in England. Patients will be able to register to access their Summary Care Record using secure HealthSpace website (NHS CfH, 2008).

In one of NHS CfH conferences in November 2007 (Thick, 2007) they presented the strategy roadmap of the NPfIT from 2000 to 2012 as it shows in (Figure 1) and they titled it "*We have a clear direction for the overall journey*." This vision includes NHS CfH plan about "reform" journey, centre's "leadership" journey, and "service" journey. It also presents some expected key outcomes, such as:

- In the early stage of the NPfIT (around 2002): Key illnesses, throughput, and capacity.

- In a later stage (2006): Health priorities, waiting times, and financial stability.
- In the semi-final stage (2010): Quality, safety, responsiveness, and joint up care.
- In the final stage (2012): Health, well-being and equity.

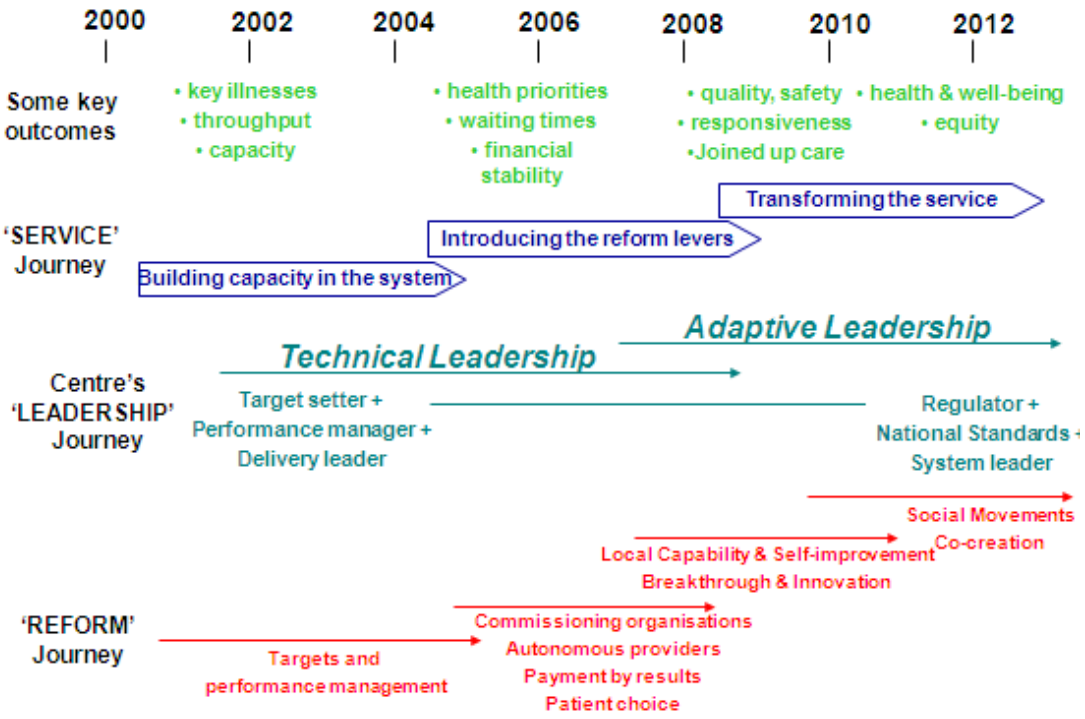

Figure 1. The direction of the overall journey of the NPfIT (Thick, 2007)

4 CARE RECORD SERVICE (CRS) DESIGN

NHS CRS is designed, according to NHS CfH, to enable each person's detailed records to be securely shared between different parts of the local NHS, such as the GP surgery and hospital. The access process design as proposed by NHS CfH is shown in (Figure 2).

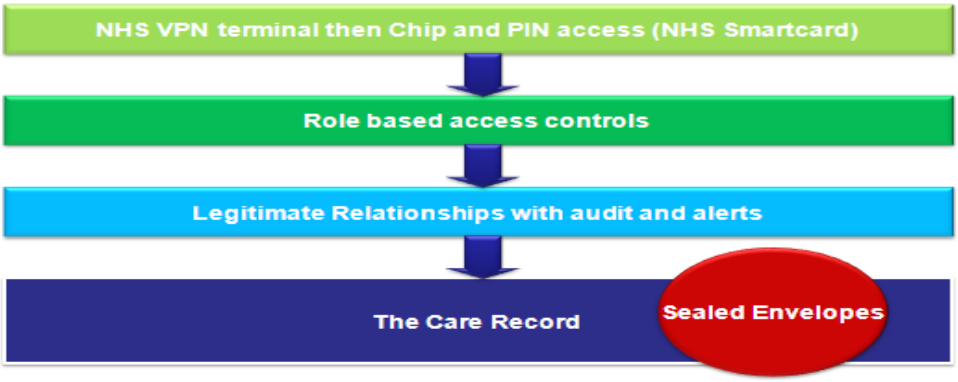

Figure 2. The access process (Eccles, 2007)

NHS health carers will be able to access patients' health records by using their NHS smart cards with chip and pin access mechanism through NHS VPN terminal.

Access will be granted according to role-based access controls with legitimate relationships between health carers and patients. With this process, an audit and alert procedures will be running to access the care records of patients.

To limit access to sensitive data, NHS CfH proposed a mechanism to ensure confidentiality of patients' information within the NHS Care Record Service which they called it "sealed envelopes", it is going to be explained in more details later. NHS CfH plan to obtain a secure shared electronic health records system was presented in different NHS CfH events such as (meetings, conferences and workshops), and in different (documents, leaflets, CDs and brochures).

4.1 NHS smartcard

A smartcard is a creditcard-sized plastic card, containing an electronic chip for security. It is printed with the health carer name, photograph and unique identity number (UUID).

Each Trust is responsible for setting up a Registration Authority (RA) to issue NHS smartcards and manage the registration process.

The registration process was set to ensure:

- Identity is confirmed beyond reasonable doubt to a government recommended standard (e-GIF level 3) (Cabinet Office, 2010).
- Allocated access control according to job role and duties.
- Passcode is set by individual, which must not be shared.

4.2 National Network for the NHS (N3)

British Telecommunication (BT) was awarded the National NHS Network (N3) contract on February 19th 2004 and acts as a network integrator. The service replaces NHSnet.

Primary Care Trusts (PCTs) and practices can get branch practices connected to the network and use the National NHS Network (N3) Virtual Privet Network (VPN) services to provide a secure network between GP practice and its branch surgeries.

4.3 Access Control

Access to NHS CRS data (held by the Personal Spine Information Service) is controlled by the Access Control Framework which registers and authenticates all users.

It will provide a single log-in and a record of each healthcare professional accessing a patient's NHS Care Record. All information will be provided on a need-to-know basis and based on a user's role and 'legitimate relationship' with the patient.

It will store details of those relationships between healthcare professionals and patients, as well as patient preferences on information sharing (e.g. whether certain sensitive information is restricted from routine sharing).

4.4 Legitimate Relationship

Legitimate Relationship is the concept of only allowing NHS health carers to access patient clinical data with the view to providing healthcare. A 'Legitimate Relationship' (LR) reflects the fact that a member of staff from a service organisation may be involved in the care and treatment of a particular patient, or has some other direct relationship with the patient that justifies access to that patient's records.

The Legitimate Relationship Service (LRS) provides a mechanism for setting up and maintaining legitimate relationships between NHS personnel and patients. The LRS is a centrally managed service residing on the BT N3 network and applications which are part of the NHS Care Records Service (NCRS) must utilise it in order to comply with NHS CfH Access Control Framework (ACF) guidance. An NCRS user is unable to access a patient's clinical record without a Legitimate Relationship.

A Legitimate Relationship will normally be created transparently for a user as part of the usual workflow within NCRS applications, for example, when a GP refers a patient to a hospital clinic, the recipient application will automatically create a Legitimate Relationship (in this case it is a Referral LR that is created) for the Workgroup associated with the clinic team.

4.5 Alerts

Alerts are used to alert a privacy officer in a healthcare organisation in situation where there is questionable appropriateness of user access.

4.6 Audit trails

Records made when a patient's record is accessed, which are available to patients on request and to privacy officers for investigative purposes.

4.7 Sealed Envelopes

Sealed Envelopes is a mechanism was proposed by NHS CfH to ensure different access control levels when the detailed health record system is in place. This access mechanism assumes that patients, and/or their authorised representative(s), in consultation with their clinician(s), will be able to (NHS CfH, 2006b):

- Identify one or more sets of sensitive information, see (Figure 3) for different sets of EHR systems, which should be sealed from everyone other than the author and people in the same Workgroup as the sealer;
- For each set of sealed information, decide whether people other than the author and those in the same Workgroup as the sealer could ever gain access:
    - If "sealed", the information could be made available to users outside the Workgroup with the patient's permission, or through override in exceptional circumstances (e.g. public interest); or
    - If "sealed and locked", users from outside the Workgroup would be unaware that the sealed information existed;
- change their minds at any time and change or remove one or more of the restrictions.

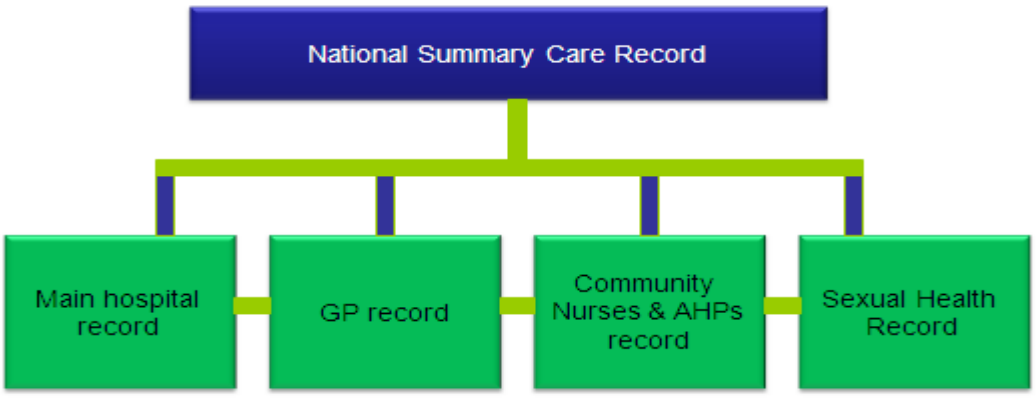

Figure 3. Sharing between different EHR systems (Eccles, 2007)

4.8 The consent model

In the SCR, the approach for individuals to participate is on an opt-out basis. That means that the patient's record would be uploaded to the spine unless the patient actively did something to indicate otherwise.

The advantage of the opt-out approach is that a greater coverage of the health system will be achieved and more people will end up on the system. In addition, more comprehensive data will be available for health care. The disadvantage is that the patient doesn't make an active choice to make his/her health record available on the system (Health Connect program Office, 2002).

When the programme was implemented, patients were given three options to store and share their EHR information; these options are:

- **Store and share**: This option is available to clinicians via SCR which is visible to an authorised user, with legitimate relationship to that patient. For patients, their SCRs are visible to them via HealthSpace.

Store but don't share: For clinicians, SCR will exist but will not be automatically visible to any authorized user. The patient may give a clinician permission to override the share status and view the record. The status can only be overridden with a court order or statute. For patients, SCRs are visible to them via HealthSpace.

Don't store and don't share: This occurs when the patient decides to opt out. For clinicians, via SCR, a blank summary is created, stating that the patient didn't want to have a SCR. Even if the consent status is changed to share, no data is available to be viewed. For patients, via HealthSpace, no clinical data is available. A note confirming this choice is visible.

These options were changed after the first year independent evaluation for early adopters of the SCR in (2008) to be only two choices:

Store but don't share: In this case, consent is requested in order to view, patients need to give their consent at every time a clinician needs to access to the patient's record.

Don't store and don't share: This is when patient decides to opt out of the national system.

The Care Record Service (CRS) in England is designed to have different sharing levels. Each sharing level is supposed to have different consent mechanisms.

When records are being shared within the clinical department, different information from different sets is being shared. For instance, three sets of information are shared:

a) The clinical notes investigations, results, and treatment.
b) Administrative record and demographics information.
c) Administrative record, appointments and letters.

The consent to access and share this information in this case is implicit because the three sets of information exist in the same record system.

When the records are being shared within an Acute Trust, which is a secondary care organisation, usually three different record sets are being shared mainly:

a) Investigations and results with labs/other departments
b) Treatments with pharmacy and other departments
c) Anonymous activity reporting to Trust management

The consent to access and share this information in this case is implicit even if the three sets of records exist in separate record systems and could be integrated in one clinical notes system.

The consent to access and share information is explicit, when clinical records are being shared outside the provider organisation, as when sharing is between:

a) General Practice.
b) Statutory grounds (consent is not essential).
c) Other healthcare providers.
d) Referrals to secondary/tertiary care.

Clinical records are anonymised and the consent to access and share the information is implicit when clinical records are accessed and shared with other organisations and for different uses, such as:

a) Epidemiology
b) Commissioners
c) Secondary Uses Service (SUS)

5 RELEVANT DOCUMENTS

5.1 Information Governance

NHS CfH website (http://www.connectingforhealth.nhs.uk/) provides information about what Information Governance is and what it includes.

It defines the Information Governance (IG) mission, which is to ensure necessary safeguards for, and appropriate use of, patient and personal information. IG includes key areas, which are:

- information policy for health and social care,
- IG standards for NPfIT systems
- and development of guidance for NHS and partner organisations.

The Information Governance Statement of Compliance (IGSoC) is "*the agreement between NHS CfH and Approved Service Recipients that sets out the terms and conditions for use of NHS Connecting for Health services, including the N3 network, in order to preserve the integrity of those services whether this use is directly or indirectly"* (NHS CfH, 2007).

A published document, called "IG Toolkit" (DoH, 2007) should be considered, which includes Information Governance standards and guidance for the NHS and partner organisations.

NHS IG defines confidentiality in terms of:

- standards of practice for confidentiality, and
- patient consent to information sharing.

IG assures that health records are confidential as they should be shared only on a need-to-know basis. NHS CfH introduced national standards so that all of its systems can protect the confidentiality of patient information and provide access to relevant information to those who need it. For this reason IG considered two key patient confidentiality issues:

-Patient choices: which is mainly information on some of the choices available to patients to control access to confidential information; and

-Information Governance alerts: where are triggered when specialist staff need to be informed of questionable access, and there is someone viewing a confidential patient record and he is not entitled to do so.

IG Toolkit listed different documents that guard information sharing in EHR systems. These documents are:

5.2 The Care Record Guarantee

This document describes how patient information is protected and used. The NHS (National Health Service) Care Record Service (CRS) in England set the Care Record Guarantee to form an important part of the public information campaign about NHS Care Records and to cover people's access to their own records, controls on others' access, how access will be monitored and policed, options people have to further limit access, access in an emergency, and what happens when someone cannot make decisions for themselves. However, this document is still general and it looks at how access rights should be. It does not explain the details of how to keep these records confidential and secure in case of intended abuse. Hence, a well-defined security strategy that is acceptable to all key stakeholders is lacking.

5.3 Standards and guidance

NHS CfH has a range of standards to ensure that information is processed securely and with proper regard for its confidentiality, integrity and availability.

NHS CfH recommends the ISO 27000 series to be used in practice which is shown in (Table 1). These standards have been specifically retained by the International Standards Organisation (ISO) for information security issues. The ISO 27000 series includes a range of individual standards, each one targets various information security controls (NHS CfH, 2010). The aim of the ISO 27001 standard is to "*provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System*" within the context of the organisation's overall business risks. This standard was published in October 2005, essentially replacing and enhancing the content of the old BS7799-2 standard. The ISO 27001 standard defines its process approach as "*The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management*". It employs the PDCA, Plan-Do-Check-Act model to structure the processes (NHS CfH, 2010).

Standard	**Standard description**
ISO 27001	This is the specification for an information security management system (an ISMS) and replaces the old BS7799-2.
ISO 27002	This is the potential new standard number of the existing ISO 17799 standard (which itself was formerly known as BS7799-1) and outlines a

	code of practice for information security.
ISO 27003	This will be the official number of a new standard intended to offer guidance for the implementation of an ISMS (IS Management System).
ISO 27004	This is the designated number for a new standard covering information security system management measurement and metrics.
ISO 27005	This is the ISO number assigned for an emerging standard for information security risk management.
ISO 27006	This standard will provide guidelines for the accreditation of organizations offering ISMS certification.

Table 1. ISO 27000 series

ISO 27001 is applicable to all types of organisations consuming NHS CfH digital services and who have an N3 connection (e.g. Acute Trusts, Foundation Trusts, County/City Councils, GPs, Commercial Enterprises, Government Agencies, not-for profit organisations). It defines requirements for the implementation of security controls customised to the needs of individual organisations or parts therefore. The standard considers the protection of critical information, such as in the health sector (NHS CfH, 2010).

The standard should be supported by the entire organisation through education, training, communication and awareness of comprehensive security policies and procedures, and should be controlled by professionals who are responsible for Information Governance within the organisation, either the health organisation or the technology and networking provider organisation. ISO 27001 is also highly effective for organisations which manage information on behalf of others, such as IT outsourcing companies. It can be used to assure customers that their information is being protected (NHS CfH, 2010).

5.4 Legal Acts

A list of relevant legal acts is shown in (Table 2) that concerns sharing medical information and accessing health records.

The Legal Act	**Date**
The Public Records Act	1958
The Access to Medical Reports Act	1988
The Access to Health Records Act	1990
The Computer Misuse Act	1990
The Data Protection Act (DPA)	1998

The Data Protection (Processing of Sensitive Personal Data) Order	2000
The Electronic Communications Act	2000
The Freedom of Information (FOI) Act	2000
The Privacy and Electronic Communications (EC Directive) Regulations	2003
The National Health Service Act	2006

Table 2. Relevant legal Acts

Data Protection Act (1998) defines health information as "personal data", and health records are considered to be under "accessible records". In this Act, in Schedule 3, Section 4(3), for processing of sensitive personal data, that the data subject (the patient) has to give his/her explicit consent to the processing of his/her personal data, and access process must be carried out in the course of its legitimate activities by anybody. However, in the same section, Article 8 says that if it is necessary for medical purposes, access process is allowed by a health professional without explicit consent.

On the other hand, Freedom of Information Act (2000) exempts sharing some information, such as health and safety information and personal information. While the Access to Health Records Act (1990) includes provisions about:

- Right of access to health records.
- Cases where right of access may be wholly excluded.
- Cases where right to access may be partially excluded.
- Correction of inaccurate health records.
- Duty of health service bodies to take advice.

The Access to Medical Reports Act 1988 allows individuals to see medical reports. However, in certain circumstances the patient may be prohibited from viewing all or part of the report if:

- In the opinion of the doctor, viewing the report may cause serious harm to the patient.
- Access to the report would disclose third-party information.

6 CONCLUSION:

The NPfIT doesn't have a single document for information security strategy, but there are different information security artefacts (documents, presentations, etc.) that are being presented in different occasions such as access control, sealed envelopes, consent mechanisms and different standards and legal Acts that govern information security and information sharing protocols in general and in the health sector in particular. This paper has attempted to put together and to make some sense out of the different information security artefacts that have been published, discussed, or proposed in the NPfIT.

The different information security issues were highlighted to understand the NPfIT information security strategy.

This paper has provided a comprehensive vision about information security strategy of one of the biggest EHR systems in the world. This strategy could be adopted and improved to fit with different EHR systems.

References

Cabinet Office (2010) *e-GIF*, url: http://www.cabinetoffice.gov.uk/govtalk/faqs/egif.aspx

Crespin, P. Miller, C. and Batteau, A. (2005) 'Ethnographic research methods'. In Swanson, R. and Holton, E. (2005) *Research on organisations: Foundations and methods of inquiry*, Barrett-Koehler Publishers, San Francisco, California, USA.

DoH, Department of Health (2007) NHS Information Governance – Guidance on Legal and Professional Obligations, September, Gateway reference 8523

Eccles, S. (2007) 'Safeguards for sharing: what the National Programme for IT is providing', *NHS CfH Conference on: The Future for Information Sharing in Sexual and Reproductive Health: Making I.T. Work*, 15 March, London.

Health Connect program Office (2002) 'Consent and Electronic Health Records: A discussion paper', *A health information network for all Aust*ralians, Australia, July.

Hayrinen, K. Saranto, K. and Nykanen, P. (2008) 'Definition, structure, content, use and impact of electronic health records: A review of the research literature', *International Journal of Medical Informatics*, vol. 77, pp. 291-304.

Myers, M. (1999) 'Investigating information systems with ethnographic research', *Journal of Communications of the Association for Information Systems*, vol. 2, Article 23.

NAO National Audit Office, Department of Health (2006) *The National Programme for IT in the NHS*, report by the Comptroller and Auditor General, HC 1173 Session 2005-2006.

NHS CfH (2010) Introduction to ISO 27000, url:
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/standards/iso27000

NHS CfH (2008) *Supporting Transformation: A practical guide to NHS Connecting for Health*, url:
http://www.connectingforhealth.nhs.uk/engagement/public/partnerships/voluntary/governance/pracguide.pdf

NHS CfH (2007) *IGSoC information pack*, url:
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/links/infopack.pdf

Orlikowski, W. (1991) 'Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology', *Journal of Accounting, Management and Information Technologies*, vol.1, pp. 9-42.

Purser, S. (2004) *A practical guide to managing information security*, Artech House, Boston. London.

Thick, M. (2007)' The Clinical Office: one year on', *Annual NHS Connecting for Health Clinicians Conference*, 15 November.