*Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services*

Contract 2013 63 02

# Overview of the national laws on electronic health records in the EU Member States

## National Report for United Kingdom (England)

March 2014

This Report has been prepared by Milieu Ltd and Time.lex under Contract 2013 63 02.

This report was completed by Carlisle George. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Executive Agency for Health and Consumers

Milieu Ltd. (Belgium), rue Blanche 15, B-1050 Brussels, tel: +32 2 506 1000; fax: +32 2 514 3603; florent.pelsy@milieu.be; web address: www.milieu.be

# Executive Summary

## 1. Stage of development of EHRs in UK (England)

The United Kingdom (UK) consists of four home countries namely England, Scotland, Wales and Northern Ireland, each having a separate national health system. These national health systems have various types of electronic health records (EHRs) and each country has its national information governance structure. In order to narrow the scope of this report, the major emphasis will focus on EHRs in England, with some reference made to the other UK countries. Two main categories of EHRs are discussed namely: detailed EHRs used by General Practitioners (GPs) or hospitals and summary EHRs records (accessed nationally and used for emergency and out-of-hours care).

In England, the National Health Service (NHS) Summary Care Record (SCR) was first introduced nationally in 2008. The SCR is stored (as read-only pdf files) on a central NHS computer (the NHS Spine) and accessed nationally (based on strict access control measures) by authorised healthcare staff. To date (2014) over 34 million SCRs have been created.

Similar national summary records exist in the other three UK countries. Scotland has three different national summary records: The Emergency Care Summary (ECS) launched in 2006; the electronic Palliative Care Summary (ePCS) record in 2009; and the Key Information Summary (KIS) in 2013. In Wales the Individual Health Record (IHR) was implemented in 2005. In Northern Ireland the Emergency Care Summary (ECS) was introduced in 2008 and the Northern Ireland Electronic Care Record (NIECR) in 2013.

## 2. Summary of legal requirements applying to EHRs

In England, there is no legislation governing EHRs specifically. Legislation and regulations pertaining to health and medical practice make reference to medical records (meaning both paper and computerised/electronic forms). There are, however, a few legislative provisions that apply specifically to electronic medium, for example, legislation regulating the type of IT systems that GPs can use in their practice or legislation pertaining to ePrescribing. Various pieces of legislation, common law, standards and guidance, form an Informance Governance framework that regulates health care and health care professionals.

GP and hospitals records contain all relevant (detailed) information relating to the treatment of a patient. Although in hospitals there is a requirement that mental health notes are kept separate from acute notes. In England, the summary record (accessed nationally for out-of-hours and emergency care) is created by extracting a subset of information from the detail record held by a GP. For example in England the SCR will only contain a patient's medications, adverse reactions and allergies (core information). Additional information can be added to the SCR with the consent of the patient, however, some types of data are automatically excluded because they are considered too sensitive (e.g. HIV AIDs data or sexual disease, termination of pregnancy).

In order for an institution (GP or Hospital) in England to host medical records including EHRs, it must hold an appropriate licence and be subject to NHS contractual conditions. The licencing requirements and contractual conditions will reflect the standards required to provide a health care service and to host medical records whether in paper or electronic form. Where medical records are computerised they must conform to certain standards (e.g. approved IT systems). Institutions must also have an information governance framework in place that will cover various issues including: management structures and responsibilities; staff training; confidentiality and data protection; and information security.

With regard to consent, GP and hospital records (whether in paper or electronic form) do not require patient consent or authorisation to be created or updated. The law mandates that a medical record must be created for every patient who is seen or treated by a medical professional. According to the Caldicott Principles (on information governance) implicit consent to the sharing of patient information is only applicable in instances of direct care, and only relevant information should be shared between professionals in support of their care. Further consent should be obtained before sharing a patient's whole care record with other registered and regulated health and social care professionals for the purposes of direct care. With regard to summary records (accessed nationally), in England, a patient is first informed about the creation of an SCR, and provided that he/she does not opt-out, the SCR is automatically created. SCRs are therefore created by implicit consent. Patient consent is required every time an SCR needs to be accessed, however, in certain situations when a patient is unable to give consent an SCR can be accessed. Patients must also explicitly consent to changes in categories of information stored in their SCR.

After any kind of EHR (GP/Hospital/Summary) has been created, generally patients are allowed to view it by making a subject request under the UK Data Protection Act 1998. However, information contained in an EHR (or any medical record) need not be disclosed if it would be likely to cause serious harm to the physical or mental health of the data subject or any other person. Patients cannot update their EHR. GP EHRs can be accessed and updated by the GP and authorised staff in the GP practice (such as nurses, health care assistants and administration staff). Hospital records can be accessed and updated by medical professionals who are directly caring for a patient and other authorised staff. In England, an SCR is hosted on a national NHS computer network (in pdf format) and accessed by medical professionals in organisations authorised to access this network. Such organisations must have information governance processes in place. Access to the SCR can only take place using an NHS smartcard (with a chip and passcode). All access is based on the particular role of the accesser (e.g. clinical information will only be accessible to clinicians). An SCR is updated at a patient's GP practice.

There is no specific liability in law related to EHRs per se, however, liability can apply to medical records in any form (whether EHRs or paper based records). EHRs and paper records are treated equally in existing legislation. There is liability in law (e.g. medical negligence), liability in terms of professional conduct and liability in terms of contractual obligations. With EHRs, however, due to the possibility of system malfunction and failure, there is the need to consider liability related to business continuity.

In relation to secondary use, in England, the Health and Social Care Information Centre (HSCIC) is empowered by law to collect medical information from GP practices for secondary uses. The HSCIC has a Secondary Uses Service (SUS) that is the single, comprehensive repository for health care data in England. The SUS enables a range of reporting and analyses to support the NHS in the delivery of health care services. Patients have a right to object to any personal confidential data being extracted unless there is a statutory duty to share information, a court order or an overriding public interest in disclosure. Categories of information collected include: ethnicity and any data from the previous four months about referrals, prescriptions or health information such as diagnoses. Categories of information not collected include: codes that relate to sensitive information including HIV/AIDS, sexually transmitted infections, termination of pregnancy, IVF treatment, marital status, complaints, convictions, imprisonment, and abuse by others.

The archiving of EHRs is subject to the Data Protection Act 1998, Principle 5 which states that: 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'. However GPs have been advised that their EHRs are needed especially to provide medico-legal evidence (e.g. to establish or refute allegations of negligence or poor performance) and should be retained indefinitely by a practice, as they are the sole source of forensic evidence. SCRs are archived and retained indefinitely as historical documents.

With regard to data requirements and interoperability, GPs and hospitals are not mandated to have one common IT system, but can choose from various commercial IT system providers. Specific requirements for the type of computerised systems used are mandated in NHS contact documents. Different medical institutions also use different systems for coding medical information, however, by 2015, in England, all NHS staff (or staff at any organisation who deliver care on behalf of the NHS) interacting with patients should use the SNOMED CT coding system to record and exchange coded clinical information.

In England, the EHRs and the Electronic Prescription Service (EPS) are fully integrated. Both the EHR and ePrescription are part of one system. The ePrescription consists of an electronic message that is created using information contained in an EHR,in addition to details of the medication prescribed. The electronic message is then sent to the EPS which makes the message available to dispensers. An EHR and ePrescription are linked via a unique patient identifiable number, for example, the NHS number in England.

## 3. Good practices

There is an exclusion data set for the SCR that protects sensitive information about the patient such as data on HIV aids or sexual diseases and pregnancy terminations. There is also a governance process around any decisions about including information from other sources into an SCR. In particular a content and advisory board has been established to examine requests for any information from other sources (other than GP records) to be included in an SCR.

Institutions that host EHRs must have an appropriate licence and are subject to NHS contractual requirements and information governance standards. From a data protection perspective, institutions that host EHRs will be data controllers and as such will have to meet the requirements of data protection legislation.

Good guidance for when implicit and explicit consent is required for sharing patient data is given in various policy documents and in particular the 2013 revised Caldicotte principles. The application of the common law duty of confidence means that unless patient information is being used for the direct care of a patient, then in most cases consent is required. This requirement, however, can be set aside only by the Secretary of State after a heavily scrutinised process. Use of implicit consent (rather than an opt-in explicit consent model) to create SCRs enables a greater number of SCRs to be created. Due to the sensitivity of the information in an SCR (and the ability for it to be accessed nationally) it is an essential requirement that consent is asked for each access to an SCR (unlike for hospital or GP records). However, the regulations also allow for access without permission in certain defined cases. The Information Commissioner's Office (ICO) ensures very effective regulation and compliance with data protection requirements including consent.

Access to an SCR via smartcard use with chip and pin works well for a number of reasons. There is a very robust process for authenticating users and issuing smart cards. They can only be issued by a named registration authority that verifies identities via official documentation such as passports. Each smart card is unique to an individual user. Also there is an ability to audit the use of smart cards. Each use of a smart card is electronically documented and can be traced back to the owner of the smart card. Various factors militate against the sharing of smart cards, such as legislation, employment policies and disciplinary processes. There is a unique identifier for each individual user, who is liable for any access in their name. All organisations must have a privacy officer and he must be trained to interrogate the relevant technical systems to investigate any allegations of inappropriate access to records.

To militate against medical liability, in hospitals, regular internal and external audits are made to demonstrate compliance with NHS regulations and standards. Reminders on hospital screen savers are used to give staff advice on how to use medical information and the consequences of misuse. All new hospital staff need to complete information governance training before they are allowed to access any

system. Also all hospital staff need to undergo mandatory information governance training once a year.

Although the HSCIC is empowered to collect patient data from GP surgeries and health care providers (for secondary uses), patients have a right to object to any personal confidential data being extracted unless there is a statutory duty to share information, a court order or an overriding public interest in disclosure. There are also limitations on the kinds of medical information that will be collected from GP medical records for secondary uses by the HSCIC. In particular, sensitive information including HIV/AIDS, sexually transmitted infections, termination of pregnancy, IVF treatment, marital status, complaints, convictions, imprisonment, and abuse by others will not be collected.

Data protection legislation requires that data is not kept for longer than necessary,. In practice this means that in some circumstances it may be that personal data can only be retained for a short period, and in other situations indefinite retention can be justified. The advice given to GPs is that EHRs should be retained indefinitely (by a GP) to provide medico-legal evidence as they are the sole source of forensic evidence. SCRs are kept indefinitely.

With regarding to interoperability, the setting up of the 'GP Systems of Choice' funding organisation ensures that although GPs can procure different IT systems there will be certain guaranteed standards. Also by 2015 all NHS staff (or staff at any organisation who deliver care on behalf of the NHS) interacting with patients should use SNOMED CT to record and exchange coded clinical information.

The EHR and ePrescription systems are fully integrated systems, and the EHR and an ePrescription are linked by a unique patient identifier to ensure that an ePrescription is for one particular patient.

## 4. Legal Barriers

The absence of more categories of data in the SCR (and other shared electronic health records), e.g. social personal care data (as is already the case in some other UK countries, such as the ePCS in Scotland) may limit the use of an SCR. There may be need for a clinician to know personal information such as details of family members, preferred place of death, and religious affiliation.

With regarding to hosting EHRs, the lack of any specific legal requirement for use of a common IT system in medical settings (although guidelines exists for preferred IT systems) means that different types of EHRs may be developed in different hospitals (and therefore there may be difficulties in electronic sharing and interoperability). The lack of any legal obligation to use the same codes for medical data in IT systems in European member states will impact on interoperability and sharing across borders. Different countries with different users have developed their own different coding systems.

The need for patient consent for each access to an SCR can impede access. However this has to be balanced by the sensitivity and confidentiality of medical information. Sometimes there are practical difficulties in patients giving informed consent – that is, the patient must know the proposed uses and disclosure purposes of personal data. Further there is a difficulty regarding Directive 95/46/EC (EU Data Protection Directive) in terms of the definition of consent and how consent is use in the Directive itself, i.e. the qualification of consent in the preamble and in articles such as 'unqualified', 'explicit' and 'free and informed'. There is lack of clarity as to whether in each article, a different meaning is intended. There should be a single definition, unless different constructions are intended.

The need for physical smartcards to access the SCR means that access is only available to NHS (England) staff and that the SCR cannot be shared across borders or even between the UK home countries. This has implications for patient mobility even within the UK.

The move towards centralised databases of electronic health records marks a fundamental shift in the paradigm of professional responsibility for the security of patient data and about decisions to share

such data. Doctors have traditionally acted as custodians of health information, sharing relevant details with others providing care and making decisions to share information with others, with or without patients' consent. The centralisation of data on shared-access databases shifts many of these responsibilities onto the person accessing the data. It is inherently more difficult for the person accessing records to know what is relevant to their role, and therefore restrict or avoid unnecessary invasion of the patient's privacy. EU law makers need to develop legislation that reflects the new paradigm without unnecessarily stifling initiatives that promise improvements in the quality, safety and timeliness of healthcare services.

There is no specific legal liability for use of EHRs per se. This may be considered a legal barrier in terms of the law not providing certainty with regarding to the scope the extent of the liability of professionals using EHRs, since there may be particular issues with use of records in electronic form. There may be need for legal and robust contractual provisions about the responsibilities of parties (IT systems suppliers and users) especially to address liability in the event of failure. This relates to the issue of legal certainty for business continuity – how to cater for system malfunction and failure (e.g. proper testing, having regular archiving in the case of data loss) and who bears responsibility for what.

There is a lack of legal clarity with regard to archiving duration of EHRs. On one hand data protection legislation states that data should not be kept for longer than is necessary. On the other hand there is a recommendation to GPs that EHRs are needed especially to provide medico-legal evidence, therefore, both the audit trail and the associated EHR should be retained indefinitely by a practice as they are the sole source of forensic evidence.

There is no specific legal requirement for interoperability of EHRs except that preferences for the kinds of IT systems that should be used by GPs are given and in 2015 all NHS staff are required to use the SNOMED CT system to record and exchange coded clinical information. As previously noted, there are several different commercial providers of EHR IT systems in the UK.

While EHR and the ePrescriptions systems are fully integrated systems, there is no legal requirement that an EHR is a precondition for the creation of an ePrescription (although in most cases an EHR will be present).

There are some challenges relating to the transfer of data for patients seeking medical care outside their home country (Member State). The challenges involved in this include differences in the implementation of Directive 95/46/EC (in EU Member States), and the permissible variation in national law and societal norms that underpin different approaches to data protection, respect for privacy and rules for professionals.

# Contents

## List of abbreviations

| | |
|---|---|
| CCG | Clinical Commissioning Groups |
| ECS | Emergency Care Summary |
| EHRs | Electronic Health Records |
| EPS | Electronic Prescription Service |
| EU | European Union |
| ePCS | Electronic Palliative Care Summary |
| GP | General Practice/Practitioner |
| HSC | Health and Social Care Service |
| HSCIC | Health and Social Care Information Centre |
| ICO | Information Commissioner's Office |
| IHR | Individual Health Record |
| KIS | Key Information Summary |
| NHS | National Health Service |
| NHSWIS | NHS Wales Informatics Service |
| NIECR | Northern Ireland Electronic Care Record |
| SCR | Summary Care Record |
| SEPR | Shared Electronic Patient Records |
| SNOMED CT | Systematized Nomenclature of Medicine Clinical Terms |
| UK | United Kingdom |

# 1. General context

The United Kingdom (UK) consists of four countries namely England, Scotland, Wales and Northern Ireland, each having a separate national health system. All of these national health systems have various types of electronic health records (EHRs) and each country has its national information governance structure. In order to narrow the scope of this report, the major emphasis will focus on England with references made to national summary records in the other UK countries when necessary.

## 1.1. EHR systems in place

This report focuses on two main categories of EHRs that are currently in place in the UK particularly in England. The first category consists of records containing detailed patient medical records that are stored locally on information technology (IT) systems where patients receive care, i.e. in General Practitioner's (GP) surgeries or hospitals. These records will generally have similar standards across the countries in terms of their contents, i.e. information necessary for a physician to discharge his medical duties such as patient demographic data, diagnoses and medical tests results among others. In some cases medical records may also contain information on social care. Shared access to these records across various clinical settings where a patient receives care is now possible, as seen for example with the SystmOne[1] clinical computer system that can allow clinicians in different care locations (GP, district nurse, smoking clinic) to share medical records. At the time of writing there are on-going initiatives to develop other kinds of sharable EHRs, for example NHS England have a vision to develop a fully integrated digital patient record that can be used across all NHS care providers in hospitals and other settings by 2018[2].

The second category of EHRs consists of national summary records created with a limited amount of patient data obtained from the detailed medical records held by a patient's GP. These summary records are created for emergency and out-of-hours care and are accessible nationally by authorised healthcare organisations/personnel. Different kinds of national summary records exist in each UK country.

***England***

In England, the National Health Service (NHS) Summary Care Record (SCR) was first introduced by six early Adopter Care Trusts (now called Clinical Commissioning Groups) in 2007, and rolled out nationally in mid-2008[3]. The SCR is stored (as read-only pdf files) on a central NHS computer (the NHS Spine) and accessed nationally (based on strict access control measures) by authorised healthcare staff. To date (2014) over 34 million SCRs have been created[4].

***Scotland, Wales and Northern Ireland***

In Scotland the Emergency Care Summary (ECS)[5] was launched in 2006. Initially access to an ECS was restricted to hospital emergency departments and out-of-hours services, but in 2013 it was extended to be used in scheduled care to support medicines reconciliation[6]. In 2009, Scotland introduced the electronic Palliative Care Summary (ePCS) record to be used in GP practices and out-

[1] For example see: Your electronic patient record and the sharing of information: A patient's guide. http://www.tpp-uk.com/wp-content/uploads/2013/10/Enhanced-DSM-3.01-model-A-guide-for-patients.pdf (last access February 2014)

[2] SAFER HOSPITALS SAFER WARDS: Achieving an integrated digital care record http://www.england.nhs.uk/wp-content/uploads/2013/07/safer-hosp-safer-wards.pdf (last access February 2014)

[3] ibid p.4 to 6.

[4] Key statistics for Summary Care Records, http://systems.hscic.gov.uk/scr/staff/aboutscr/benefits/scrkey (last access February 2014)

[5] National Information Systems Group, Emergency Care Summary, available at http://www.nisg.scot.nhs.uk/currently-supporting/emergency-care-summary (last access February 2014)

[6] Scotland extends use of ECS, available at http://www.ehi.co.uk/news/ehi/8018/scotland-extends-use-of-ecs (last access February 2014)

of-hours care. Palliative care involves care to improve the quality of life for the terminally ill or patients facing life threatening illness. The ePCS allows GP practices to build Anticipatory Care Plans and therefore allows an anticipatory versus reactive approach to care. The ECS holds and shares ePCS information. Further in 2013 the ECS was extended to create the Key Information Summary (KIS)[7]. The KIS was introduced to support patients with: anticipatory care plans, complex medical issues, long term conditions, multiple conditions, and mental health and/or communication issues. The KIS is intended for use in hospital emergency and pharmacy environments, out-of-hours care, Scottish Ambulance Service, hospices, mental health units, and approved scheduled care departments. All of the information on the ECS is included in the KIS (hence the KIS is available for all ECS users).

In Wales a national Individual Health Record (IHR)[8] was implemented in 2005 for use in out-of-hours and emergency care settings. The IHR is an extract of a patient's GP record. It is viewable-only and is held on a central repository.

In 2008, Northern Ireland Health and Social Care Service (HSC)[9] launched the Emergency Care Summary (ECS) intended for urgent care for patients attending emergency departments and after hours services, and for hospital pharmacies. In 2013, a new Northern Ireland Electronic Care Record (NIECR) was created which can be accessed by all HSC hospital trusts and GP practices in Northern Ireland.

## 1.2. Institutional setting

The UK has a system of devolved government for Scotland, Wales and Northern Ireland whereby devolved administrations (The Scottish Government, The Welsh Government and the Northern Ireland Executive) have responsibility for various domestic policy issues, including health. With regard to data protection, the UK has one single legislative act (The Data Protection Act 1998[10]) for all four countries. The Information Commissioner's Office (ICO) is the UK's independent authority responsible for overseeing the implementing of the Act[11]. It is the primary source of advice and guidance on data protection in in the field of health. The rest of this section gives a brief introduction to some of the main health authorities in England responsible for matters regarding EHRs and related IT systems. Brief summaries of the main authorities in Scotland, Wales and Northern Ireland are also given for comparison.

***England***

- *The Department of Health*

The Department of Health is a ministerial department of the UK government supported by 23 agencies and public bodies. It is responsible for making government policy for matters regarding health and social care, and for the National Health Service (NHS) in England. It has overall responsibility for health and social care in England. It also works on some matters that are not devolved to the Government of Scotland, the Government of Wales and the Northern Ireland Executive.

- *NHS England*

NHS England (NHS Commissioning Board) is an independent non-departmental public body of the Department of Health. It is responsible for the budget, planning, delivery and general running of the

[7] New electronic health record rolls out across Scotland, http://www.alliance-scotland.org.uk/news-and-events/news/2013/10/new-electronic-health-record-rolls-out-across-scotland/ (last access February 2014)
[8] Individual Health Record, Wales, available at: http://www.wales.nhs.uk/sites3/home.cfm?orgid=858 (last access February 2014)
[9] The Northern Ireland Health and Social Care Service provides both health care and social care. In England, Wales and Scotland health care is provided by the respective National Health Service (NHS) and social care by local councils.
[10] The Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents (last access February 2014)
[11] Information Commissioner's Office, http://ico.org.uk/about_us (last access February 2014)

National Health Service in England, as detailed in the Health and Social Care Act 2012[12]. The Act also created a new national health service structure (Health and Care System) in England that became operational from the 1st April 2013[13]. The main goals of NHS England are to: provide national leadership for improving outcomes and driving up the quality of care, oversee the operation of clinical commissioning groups, allocate resources to clinical commissioning groups, and commission primary care and specialist services. NHS England has the overall responsibility for implementing IT in the NHS. For example it is responsible for setting the overall vision, strategic direction, benefits and implementation of the Electronic Prescription Service.

• *Clinical Commissioning Groups*
Clinical Commissioning Groups (CCG) were established on 1st April 2013 by the Health and Social Care Act 2012. They commission[14] most of the hospital and community NHS services in the local areas for which they are responsible. They are clinically led and include all the GP groups in their geographical area. CCGs are overseen by NHS England. The management for planning and implementation of GP IT information services (EHR systems and the Electronic Prescription Service Release 2) were delegated to CCGs by NHS England[15].

• *The Health and Social Care Information Centre*
The Health and Social Care Information Centre (HSCIC) was set up as an Executive Non-Departmental Public Body (ENDPB) in April 2013 under The Health and Social Care Act 2012[16]. Among many functions it has the responsibility to 'support the delivery of IT infrastructure, information systems and standards to ensure information flows efficiently and securely across the health and social care system, to improve patient outcomes.'[17] The Summary Care Record, the Electronic Prescription Service, IT systems for GP surgeries and Hospital IT systems are among many IT systems supported by the HSCIC.

***Scotland, Wales and Northern Ireland***

• *The Scottish Government Health and Social Care Directorate*
The Scottish Government Health and Social Care Directorate[18] is responsible for allocating resources and setting the strategic direction for NHSScotland. It is also responsible for the development and implementation of health and social care policy in Scotland. NHSScotland carries out this policy and consists of a fourteen regional NHS Boards and seven Special NHS Boards.

• *NHS National Services Scotland*
The NHS National Services Scotland (NHS NSS)[19] is the common name for the Common Services Agency that provides national strategic support services and expert advice to NHS Scotland (the publicly funded healthcare system in Scotland). It contains the National Information Systems Group[20] (NISG) responsible for delivering IT solutions in the health service, including the Emergency Care Summary (ECS) record. The functions of the NISG range from initial advice, to buying or building software, to managing IT services.

[12] The Health and Social Care Act 2012, http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted (last access February 2014)
[13] Health and Care System from 1st April 2013 (England), http://www.nhs.uk/NHSEngland/thenhs/about/Pages/nhsstructure.aspx (last access February 2014)
[14] Commissioning involves deciding what services are needed, and ensuring that they are provided.
[15] Securing Excellence in GP IT Services: Operating Model, Key Facts, December 2012 http://www.england.nhs.uk/wp-content/uploads/2012/12/gp-it-facts.pdf (last access February 2014)
[16] The statutory functions and duties of the HSCIS are set out in Part 9, Chapter 2 of The Health and Social Care Act 2012, - sections 252 to 275 - and in Schedule 1. See: http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted (last access February 2014)
[17] Health and Care Information Centre, http://systems.hscic.gov.uk/ (last access February 2014)
[18] The Scottish Government Health and Social Care Directorate, http://www.scotland.gov.uk/Topics/Health/About (last access February 2014)
[19] NHS National Services Scotland, http://www.nhsnss.org/index.php (last access February 2014)
[20] The National Information Systems Group, http://www.nisg.scot.nhs.uk/ (last access February 2014)

• *The Welsh Department for Health and Social Services*
The Department for Health and Social Services is responsible for giving the Welsh Government advice on policies and strategies regarding health and social care in Wales. Its functions include making contributions to relevant legislation and providing funding to the NHS.

• *NHS Wales Informatics Service*
The NHS Wales Informatics Service[21] (NHSWIS) is responsible for the strategic development of Information and Communications Technology (ICT), delivering operational ICT services and information management. The NHSWIS was established in April 2010 by merging a number of existing organisations including: Informing Healthcare, Health Solutions Wales, the Business Services Centre IM&T element, the Corporate Health Information Programme and the Primary Care Informatics Programme.

• *The Northern Ireland Department of Health, Social Services and Public Safety*
The Department of Health, Social Services and Public Safety (DHSSPS) has a major function, to improve the health and well-being of the people of Northern Ireland. Among its responsibilities is Health and Social Care. This includes 'policy and legislation for hospitals, family practitioner services and community health and personal social services'[22]. Health and Social Care Services are responsible for implementing the various IT systems including national EHRs in Northern Ireland.

• *Northern Ireland Health and Social Care Bodies*
The Health and Social Care (Reform) Act (Northern Ireland) 2009, created new health and social care bodies, outlined their high level functions and provided the legislative framework within which they operate. These bodies work together to provide an integrated health and social care service in Northern Ireland and are ultimately accountable to the DHSSPS. Their roles and functions are fully described in the DHSSPS Framework Document 2011[23]. The bodies include: The Health and Social Care Board (HSCB); The Public Health Agency (PHA); Health and Social Care (HSC) Trusts; The Business Services Organisation (BSO); The Patient and Client Council (PCC); The Regulation and Quality Improvement Authority (RQIA); and Special Agencies.

## 1.3. Legal setting and future legal development

In England, there is no comprehensive legislation specifically focused on EHRs. General legislation pertaining to health and medical practice makes reference to both paper and computerised (electronic) medical records. There are, however, a few legislative provisions that apply specifically to electronic medium, for example, legislation regulating the type of IT systems that GPs can use in their practice or legislation pertaining to ePrescribing. Various pieces of legislation, common law, standards and guidance, form an Informance Governance framework that regulates health care including eHealth (EHRs/ePrescriptions). Some of the main legal instruments that have an impact on eHealth are discussed below.

[21] The Wales Informatics Service, http://www.wales.nhs.uk/sitesplus/956/home (last access February 2014)
[22] The Department of Health, Social Services and Public Safety, http://www.dhsspsni.gov.uk/index/about_dept.htm (last access February 2014)
[23] The Department of Health, Social Services and Public Safety, Framework Document, Version September 2011 http://www.dhsspsni.gov.uk/framework_document_september_2011.pdf

*Health and Social Care Act 2012*

The Health and Social Care Act 2012[24], sets out the authorisation requirements needed to provide a health care service in England, and therefore by extension to create and process EHRs. Chapter 3, clause 81(1) states that '*Any person who provides a health care service for the purposes of the NHS must hold a licence under this Chapter.*' Among many other things, the Act created the new health and care system in England with new organisations and associated powers. Many of these changes impact the planning, implementation and management on health information systems and EHRs. For example Part 9, Chapter 2 of the Act established The Health and Social Care Information Centre (HSCIC), responsible for various functions including collecting and analysing national health and social care data. The act empowers the HSCIC to collect medical data (in electronic form) from GP surgeries and health care services. Data on sexual health (e.g. HIV diagnosis, abortions) and written notes are excluded. However data on mental health, actual diagnoses, medications and laboratory results are included. Patients however can object to such information sharing, unless there is a statutory duty to share information, a court order or an overriding public interest in disclosure. Among numerous other functions, the HSCIC is also responsible for supporting the IT infrastructure, information systems and standards in the health and social care system.

*The National Health Service (General Medical Services Contracts) Regulations 2004*

In England, the National Health Service (General Medical Services Contracts) Regulations 2004 as amended, establishes the authority for NHS contractors (i.e. GPs, hospitals or any healthcare service provider) to create medical records including EHRs. Section 73(2) states that 'The contractor shall keep adequate records of its attendance on and treatment of its patients and shall do so — (a) on forms supplied to it for the purpose by the [the Board]; or (b) with the written consent of the [the Board], by way of computerised records, or in a combination of those two ways.' Section 73(4) as amended, sets out requirements for the type of computerised system that can be used (i.e. security measures, audit and system management functions) and the need for contractors to sign an undertaking to abide by the Good Practice Guidelines for General Practice Electronic Patient Records published by the Department of Health.

*The Public Records Act 1958*

The Public Records Act 1958[25] establishes that medical records (and all NHS records in England) are public records. The Act further sets out responsibilities for anyone who works with public records and guidance for keepers of such records. The Act also addresses issues regarding public records selected for archiving, in particular, where these records should be transferred to.

*The Common Law Duty of Confidence*

The common law duty of confidence was established in the case of *Coco v Clark [1969] R.P.C.41.* It mandates that information must be kept confidential (not disclosed) if that information is of a confidential nature (e.g. medical data given for an EHR) and is imparted in circumstances importing an obligation of confidence (e.g. given by a patient for medical care). The duty is not binding in certain circumstances, for example where a patient gives consent for disclosure, where disclosure is required/permitted by law, or where there is an overriding public interest for disclosure. The duty of confidence is important with regard to the sharing of EHRs.

*The National Health Service Act 2006*

Section 251 of the National Health Service Act 2006[26] empowers the Secretary of State to make regulations to override the common law duty of confidentiality to enable the disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent is not practical, having regard to the cost and technology available. The power can only be used to support medical purposes that are in the interests of patients or the wider public. This law is important in allowing data in EHRs to be put to secondary uses. This is especially

[24] Health and Social Care Act 2012, http://www.legislation.gov.uk/ukpga/2012/7/pdfs/ukpga_20120007_en.pdf (last access February 2014)
[25] The Public Records Act 1958, http://www.legislation.gov.uk/ukpga/Eliz2/6-7/5 (last access February 2014)
[26] National Health Service Act 2006, http://www.legislation.gov.uk/ukpga/2006/41/contents (last access February 2014)

relevant to EHRs with the introduction of care.data which is data that the HSCIC is empowered to collect nationally, for secondary use.

*Data Protection Act 1998*

The Data Protection Act 1998[27] (which transposes Directive 95/46/EC) sets out the legal framework to regulate the processing of personal data in the UK. Personal data is any data that can identify (or that can be used with other data to identify) a living individual. The Act designates health data as a special category of personal data called 'sensitive personal data' which attracts more protection and stricter conditions for processing. The Act sets out duties and responsibilities of data controllers (those who collect personal data – e.g. GP surgeries and hospitals) and rights of data subjects (e.g. patients). An important right is the right of subjects to gain access to their personal data. The Act also stipulates eight data protection principles that data controllers must comply with (subject to various exemptions) when processing personal data. The eight data principles mandate that personal data must be: processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes of processing; accurate and kept up to data; kept for no longer than necessary; processed in accordance to rights of data subjects; kept secure from unauthorised access, unlawful processing, destruction or damage; transferred to a country outside the EU only if that country has an adequate level of data protection. The Act stipulates various conditions for the processing of data which includes the consent of the data subject among others. The Act also creates various criminal offences including 'unauthorized access to data'. The Data Protection Act 1998 has a huge impact on EHRs, by serving as the general legal instrument that establishes various patient rights (e.g. access) and determines various compliance requirements for the processing of EHRs especially with regard to content, sharing, and other uses.

*The Data Protection (Processing of Sensitive Personal Data) Order 2000*

The Data Protection (Processing of Sensitive Personal Data) Order 2000[28] amended the Data Protection Act 1998 by stipulating that information need not be disclosed (to the data subject) if it would be likely to cause serious harm to the physical or mental health of the data subject or any other person.

*The Computer Misuse Act 1990*

The Computer Misuse Act 1990[29] creates three main criminal offences in the UK namely: (i) unauthorised access to programs or data held on computer (e.g. unauthorised access to an EHR); (ii) unauthorised access with intent to commit or facilitate commission of further offences (e.g. unauthorised access to data held in an EHR with intent to commit a further offence) and (iii) unauthorised acts with intent to impair operation of a computer (e.g. unauthorised access to an EHR and intentionally modifying or deleting data).

*Common Law Medical Negligence*

Proving medical negligence in the UK involves establishing a breach of duty in healthcare. This is subject to the Bolem test (*Bolam v Friern Hospital Management Committee (1957) 1 WLR 583*) modified by the Bolitho amendment (*Bolitho v. City and Hackney Health Authority [1997] 4 All ER 771*). Under the Bolem test, a doctor does not breach the legal standard of care, and is therefore not negligent, if his actions conformed to a practice supported by a body of professional opinion. Bolitho imposed a new requirement to the Bolem test: the standard proclaimed must be justified on a logical basis and must have considered the risks and benefits of competing options.

[27] The Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents (last access February 2014)
[28] The Data Protection (Processing of Sensitive Personal Data) Order 2000, http://www.legislation.gov.uk/uksi/2000/417/contents/made (last access February 2014)
[29] The Computer Misuse Act 1990, http://www.legislation.gov.uk/ukpga/1990/18/contents (last access February 2014)

*The National Health Service (Venereal Diseases) Regulations 1974, The NHS Trusts (Venereal Diseases) Directions 1991 and The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000.*

These Acts mandate that health authorities must not disclose any information that could identify a patient being treated for sexually transmitted diseases, unless it is necessary to communicate with a medical practitioner who is treating the disease or to prevent the spread of the disease. This has consequences for the content of EHRs, especially where they are shared or sharable. The General Medical Council guidance however, states that in their view '…the Regulations and Directions do not preclude disclosure if it would otherwise be lawful at common law, for example with the patient's consent or in the public interest without consent[30].'

*The Electronic Communications Act 2000*
The Electronic Communications Act 2000, among other provisions, makes digital signatures legally admissible. This allows ePrescriptions to be electronically signed, hence making them a legal document, and creating a paperless prescription service.

*The Medicines for Human Use (Prescribing) Order 2005*.
The Medicines for Human Use (Prescribing) Order 2005[31] amended the Prescription Only Medicines (Human Use) Order 1997[32] to allow a prescription to be signed by an advanced electronic signature. This facilitated the ability to sign prescriptions electronically, hence paving the way for the issuing and transfer of prescriptions solely by electronic means. In the Electronic Prescription Service Release 1, the paper version of a prescription remained the legal form of the prescription, and a parallel electronic version (not capable of being digitally signed at that time) linked to the paper version was processed electronically. The Electronic Prescription Service Release 2 enabled electronic versions of prescriptions to be digitally signed and hence become the legal form, eliminating the need for a paper version.

*The Caldicott Principles*
In 1997 the *Review of the Uses of Patient-Identifiable Information*, chaired by Dame Fiona Caldicott, devised six general principles of information governance that could be used by all NHS organisations (in England) with access to patient information. Subsequently, The Health Service Circular (HSC 1999/012[33]) mandated that each NHS organisation (with access to patient records) is required to have a 'Caldicott Guardian', to ensure information governance is effective. A Caldicott Guardian 'is a senior person responsible for protecting the confidentiality of a patient and service-user information and enabling appropriate information-sharing'[34].

Due to a growing perception that information governance was being an impediment to sharing information a review of the principles was commissioned in 2012. This lead to the publication in March 2013 of the Caldicott 2 review consisting of a revised list of Caldicott principles[35]. The original six principles were updated and a seventh principle was added. The seven new Caldicott principles are:

[30] Confidentiality: disclosing information about serious communicable diseases http://www.gmc-uk.org/Confidentiality__disclosing_information_SCD_Revised_2013.pdf_52101285.pdf (last access February 2014)

[31] The Medicines for Human Use (Prescribing) Order 2005, http://www.legislation.gov.uk/uksi/2005/765/contents/made (last access February 2014)

[32] Prescription Only Medicines (Human Use) Order 1997 and the Medicines act 1968 cover the sale, use and production of medicines, and includes prescribing rights.

[33] HSC 1999/012, http://systems.hscic.gov.uk/infogov/links/hsc199912.pdf (last access March 2014)

[34] Caldicott Guardians, http://systems.hscic.gov.uk/data/ods/searchtools/caldicott/index_html (last access March 2014)

[35] Information: To share or not to share? The Information Governance Review, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf (last access March 2014)

(1) Justify the purpose (i.e., use or transfer of personal confidential data);
(2) Don't use personal data unless it is absolutely necessary;
(3) Use the minimum necessary personal confidential data;
(4) Access to personal confidential data should be on a strict need-to-know basis;
(5) Everyone with access to personal confidential data should be aware of their responsibilities;
(6) Comply with the law;
(7) The duty to share information can be as important as the duty to protect patient confidentiality.

# 2. Legal requirements applying to EHRs in UK (England)

In England, EHRs are regulated by an Information Governance framework consisting of legislation, common law, standards and guidance set by the relevant authorities. There is no comprehensive body of legislation aimed specifically at EHRs. No specific legislation lists the requirements of EHRs.

## 2.1. Health data to be included in EHRs

### 2.1.1. Main findings

EHRs created by GPs, contain patient identifiable information, contact information and all necessary information relating to the care of a patient including medications (including allergies and adverse reactions), diagnosis, medical notes, and laboratory tests. Each EHR must have a unique patient identifier[36]: National Health Service (NHS) number in England and Wales, Community Health Index (CHI) number in Scotland, and Health and Social Care (HSC) number in Northern Ireland.

Summary EHRs intended for national access (for emergency and out-of-hours care) contain a limited amount of information obtained from a patient's detailed medical record held at a GP's surgery. Information on sexually transmitted diseases[37], fertility and embryology, pregnancy terminations, gender reassignment and private discussions between a patient and his/her GP are not included in these records, however, medications prescribed for any of the conditions are listed.

***England***

In England (UK), the SCR is created with patient identifiable information, details of the patient's medications, adverse reactions and allergies (core information) all copied from the patient record of his/her GP into the SCR based on implied implicit consent[38]. The SCR does not identify diseases, disorders or symptoms. Additional information such as diagnoses, test results, and end of life care plans may be added to the SCR, subject to the explicit consent of the patient[39]. The SCR is updated (time and date stamped) as the information in the General Practice record changes. The information in the SCR contains the original text that was recorded in the GP system and also SNOMED CT code used to record and exchange clinical information.

***Scotland, Wales and Northern Ireland***

In Scotland the 2006 ECS[40] contains basic patient details (name, address date of birth, a unique identification number called CHI[41]), emergency contact numbers, medicines prescribed, allergies and adverse drug reactions. This information is extracted from electronic records held locally by GPs. The 2009 ePCS[42] (introduced for patients needing palliative care both in and out of GP hours) contains information on consent for palliative data transfer, ECS information, past medical history, current diagnosis, carer details, drugs available at home, patient wishes (preferred place of care and

[36] *The National Health Service (General Medical Services Contracts) Regulations 2004* as amended (Section 74B).

[37] *The National Health Service (Venereal Diseases) Regulations 1974, The NHS Trusts (Venereal Diseases) Directions 1991 and The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000.*
These Acts (England) mandate that health authorities must not disclose any information that could identify a patient being treated for sexually transmitted diseases, unless it is necessary to communicate with a medical practitioner who is treating the disease or to prevent the spread of the disease.

[38] Clay, R (2011) Summary Care Record Scope, NHS Connecting for Health.
http://www.connectingforhealth.nhs.uk/systemsandservices/scr/documents/scrscope.pdf (last access February 2014)

[39] ibid

[40] National Information Systems Group, Emergency Care Summary, available at
http://www.nisg.scot.nhs.uk/currently-supporting/emergency-care-summary (last access February 2014)

[41] CHI means Community Health Index and used in Scotland to uniquely identify individuals for health care purposes.

[42] Electronic Palliative Care Summary (ePCS)
http://www.scotland.gov.uk/Topics/Health/Quality-Improvement-Performance/Living-Dying-Well/ePCS (last access February 2014)

DNACPR[43] decision), carer details, other agencies involved and access details, and special instructions for emergency care and treatment. The 2013 KIS[44] (introduced for patients with complex care needs, multiple conditions, and mental health and/or communication issues) contains information (obtained from a GP's medical record) on medication, allergies and diverse drug reactions (similar to the ECS) and additional information including contact details, next of kin and carer details, wishes or special instructions, and self management and anticipatory care plans (if a person has long term conditions)[45].

In Wales, information in the IHR[46] is restricted to: patient's name and address, GP practice, medication, allergies, medical problems that GP is seen about, results of recent medical tests (blood tests and x-rays).

In Northern Ireland, the 2008, ECS contains information on drugs and allergies obtained from a patient's GP. The new NIECR, introduced in 2013, contains information from the ECS and other information in existing electronic records systems from hospitals and clinics[47]. Phase 1 of the NIECR contains demographic details (name, address, gender, date of birth, Health and Care Number and GP contact details), lab tests and x-rays results, allergies, allergies, medication, and visits to hospitals (and out-of-hours centres). The NIECR can be accessed by all HSC hospital trusts and General Practices (doctor's offices) in Northern Ireland.

[43] A DNA CPR means 'do not attempt cardiopulmonary resuscitation' to ensure that the patient dies in a dignified and peaceful manner.
[44] New electronic health record rolls out across Scotland, http://www.alliance-scotland.org.uk/news-and-events/news/2013/10/new-electronic-health-record-rolls-out-across-scotland/ (last access February 2014)
[45] ibid
[46] Individual Health Record, Wales, available at: http://www.wales.nhs.uk/sites3/home.cfm?orgid=858 (last access February 2014)
[47] Northern Ireland Electronic Care Record, available at http://www.ehealthandcare.hscni.net/niecr/niecr.aspx (last access February 2014)

### 2.1.2. Table on health data

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Are there specific rules on the content of EHRs? (or regional provisions, agreements, plans?)* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012) [48] | In the four home countries GP surgeries and hospitals hold full EHRs containing detailed information on patients including the following categories of data: Personal (name, address, data of birth, marital status, occupation, ethnic origin, telephone number and hospital number); clinical (medications, allergies, diagnoses, test results etc.).<br><br>National records used in emergency and out-of-hours care generally contain less information as described below.<br><br>*England*<br>A Summary Care Record (SCR) is created with the following content: patient demographics (name, address, telephone number, NHS number) and core information consisting of: medications (acute, repeat and discontinued repeat) allergies and adverse reactions. Additional information such as significant diagnoses and care plans may be added with the explicit consent of the patient.<br><br>*Scotland*<br>The Emergency Care Record (ECR) contains basic patient details (name, address date of birth, identification number - CHI number), emergency contact numbers, medicines prescribed, allergies and adverse drug reactions. This information is extracted from electronic records held locally by GPs. Additional information can be added if agreed by patient and GP. [49]<br><br>The Palliative Care record[50] contains ECR information and also information on Anticipatory Care: information on consent for palliative data transfer, ECS information, past medical history, current diagnosis, |

[48] The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012)
[49] Emergency Care Summary, What does it mean for you?, (NHS Scotland), http://www.scotland.gov.uk/Resource/Doc/143714/0036499.pdf (last access February 2014)
[50] Electronic Palliative Care Summary (ePCS) http://www.scotland.gov.uk/Topics/Health/Quality-Improvement-Performance/Living-Dying-Well/ePCS (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | carer details, drugs available at home, patient wishes (preferred place of care and DNACPR[51] decision), carer details, other agencies involved and access details, and special instructions for emergency care and treatment.<br><br>*Wales*<br>The National Individual Health Record (IHR) is restricted to containing the following information: patient's name and address, GP practice, medication, allergies, medical problems that GP is seen about, results of recent medical tests (blood tests and x-rays). Information on sexually transmitted diseases, fertility and embryology, terminations, gender reassignment and private discussions between a patient and his/her GP is not included in an IHR. However, medications prescribed for any of the conditions in the latter will be listed in the IHR.<br><br>Northern Ireland<br>The ECS contains information on drugs and allergies obtained from a patient's GP. The NIECR contains information from the ECS and other information in existing electronic records systems from hospitals and clinics[52]. Phase 1 of the NIECR contains demographic details (name, address, gender, date of birth, Health and Care Number and GP contact details), lab tests and x-rays results, allergies, allergies, medication, and visits to hospitals (and out-of-hours centres). The NIECR can be accessed by all HSC hospital trusts and General Practices (doctor's offices) in Northern Ireland. |
| *Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012) | *England*<br>SCRs in England and other national EHRs are restricted to purely medical information. Other types of non-medical information (e.g. socio-economic situation, ethnicity) are not included. |
| *Is there a definition of EHR or patient's summary provided in the national legislation?* | *The National Health Service (General Medical Services Contracts)* | There is no generic definition of EHR however the SCR is defined in national legislation.<br>"Summary Care Record" means the system approved by the Board for the |

[51] A DNA CPR means 'do not attempt cardiopulmonary resuscitation' to ensure that the patient dies in a dignified and peaceful manner.
[52] Northern Ireland Electronic Care Record, available at http://www.ehealthandcare.hscni.net/niecr/niecr.aspx (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | *Regulations 2004* as amended Schedule 6, Section 74(3)[53] | automated uploading, storing and displaying of patient data relating to medications, allergies, adverse reactions and, where agreed with the contractor and subject to the patient's consent, any other data taken from the patient's electronic record". |
| *Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012) | As noted above first an SCR is created only with core information (Medications (Acute, Repeat and Discontinued Repeat) Allergies and Adverse reactions). After additional information can be included but only with the explicit consent of the patient. Such addition information can include significant diagnoses or care plans. |
| *Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?* | Information Standards Notice – New Standards, ISB, 2011 | The SCR does not identify diseases, disorders, symptoms. It is only a summary used for emergency and after hours care. The information in the SCR contains the original text that was recorded in the GP system and also SNOMED CT code[54]. In 2011 the Information Standards Board for Health and Social Care approved the adoption of the SNOMED CT code in England[55]. By 2015 all NHS staff (or staff at any organisation who deliver care on behalf of the NHS) interacting with patients should use SNOMED CT to record and exchange coded clinical information. |
| *Are EHRs divided into separate categories of health data with different levels of confidentiality (e.g. data related to blood type is less confidential than data related to sexual diseases)?* | | GP electronic records are not divided into separate categories.<br><br>National summary records will not contain information on sexual diseases, although they will contain medication that is used to treat sexual diseases.<br><br>Access to the content of an SCR is controlled using Role Based Access Control (RBAC). This limits the functions that can be used by a particular user. For example using RBAC a user can only be allowed to see demographic information or clinical information. |
| *Are there any specific rules on identification of patients in EHRs?* | The NHS Summary Care Record Guide for GP | All patient medical records will have a unique identifier (e.g. the NHS number in England). The SCR contains the name and NHS number of a |

[53] The National Health Service (General Medical Services Contracts and Personal Medical Services Agreements) Amendment Regulations, http://www.legislation.gov.uk/uksi/2014/465/made (last access February 2014)

[54] SNOMED CT (Systematized Nomenclature of Medicine Clinical Terms) is an internationally recognised set of numerical, machine readable codes and human readable descriptions, which can be used to uniquely identify clinical concepts. It is a standard essential for the interoperability of electronic health records across care settings. SNOMED CT is managed and maintained internationally by the International Health Terminology Standards Development Organisation (IHTSDO) and in the UK by the UK Terminology Centre (UKTC).

[55] Information Standards Notice – New Standards, ISB, 2011. Available at http://www.isb.nhs.uk/documents/isb-0034/amd-26-2006/isn.pdf (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | Practice Staff V1.2 (October 2012) | patient, data of birth. |
| *Is there is a specific identification number for eHealth purposes?* | *The National Health Service (General Medical Services Contracts) Regulations 2004* as amended (Section 74B) | *The National Health Service (General Medical Services Contracts) Regulations 2004* as amended Section 74B states that: 'A contractor must include the NHS number of a registered patient as the primary identifier in all clinical correspondence issued by the contractor which relates to that patient.'<br><br>The SCR contains the NHS number (10-digits) of a patient. It is a national unique patient identifier. Everyone registered with the NHS in England and Wales is assigned a unique NHS number. An NHS number is assigned when a patient registers with his/her GP.<br><br>Wales also uses an NHS number to uniquely identify a patient in an EHR.<br><br>In Scotland the Community Health Index (CHI) is a population register (database), which is used for health care purposes. The CHI number (Community Health Index database) has a 10 character code which uniquely identifies each patient in an EHR.<br><br>In Northern Ireland the Health and Care Number (HSC), is the Number, and is used to provide a unique patient identifier in an EHR. |

## 2.2. Requirements on the institution hosting EHRs data

### 2.2.1. Main findings

In England, national summary EHRs (i.e. SCRs) are held on a national IT infrastructure and are updated from detailed EHRs held by GP practices.

With respect to GP practices, under the *Health and Social Care Act 2012*, Chapter 3, clause 81(1) 'Any person who provides a health care service for the purposes of the NHS must hold a licence under this Chapter.'[56] The licencing requirements will reflect the standards required to provide a health care service and indirectly (but not specifically) to host EHRs.

Any contractor (GP or health care service) providing medical services to the NHS (The NHS Commissioning Board) must sign a contract with the said Board pursuant to Section 73 of *The National Health Service (General Medical Services Contracts) Regulations 2004* as amended. The requirements listed in this contract include that a medical record must be kept for any patent attended to or treated and that if the record is computerised, then that computer system must conform to certain requirements. These requirements for Section 73 of *The National Health Service (General Medical Services Contracts) Regulations 2004* as amended are reflected and updated in the most recent model *Standard General Medical Services Contract – April 2012*.[57]

With regard to staff, clause 16.2.1 states that 'The Contractor shall nominate a person with responsibility for practices and procedures relating to the confidentiality of personal data held by it.'

All NHS (England) organisations must use an information governance toolkit to assess themselves which has specific controls for the use of electronic information by health and social care organisations[58]. All organisation must assess themselves against requirements for: management structures and responsibilities (e.g. assigning responsibility for carrying out the information governance assessment, providing staff training); confidentiality and data protection; and information security[59].

With regard to encryption, *The Good Practice Guidelines for GP electronic patient records - version 4 (2011)* requires encryption where electronic data is removed from GP practice premises (Section

[56] Clause 83 however, states that regulations may grant exemptions from clause 81 for (i) a prescribed person or health care service or (ii) persons or health care services of a prescribed description.

[57] Clause 16.1.2 of the model *Standard General Medical Services Contract – April 2012* states that:

> 'The Contractor shall keep adequate records of its attendance on and treatment of its patients and shall do so-
> (a) on forms supplied to it for the purpose by the Board; or
> (b) with the written consent of the Board, by way of computerised records,
> or in a combination of those two ways'

Clause 16.1.4 contains specific requirements for the computer system used to store EHRs. It states that:

> 'The consent of the Board required by clause 16.1.2(b) shall not
> be withheld or, once given, withdrawn provided the Board is satisfied, and continues to be satisfied, that-
> (a) the computer system upon which the Contractor proposes to keep the records has been accredited by the Secretary of State or another person on his behalf in accordance with General Practice Systems of Choice Level 2;
> (b) the security measures, audit and system management functions incorporated into the computer system as accredited in accordance with sub-clause (a) have been enabled; and
> (c) the Contractor is aware of, and has signed an undertaking that it will have regard to the guidelines contained in "Good Practice Guidelines for General Practice Electronic Patient Records (version 4)" published on 21st March 2011...'

Clause 16.1.4 (b) mandates that the auditing functions of the computerised system must be enabled and functioning properly. It states that:

> 'Where a patient's records are computerised records, the Contractor must, as soon as possible following a request from the Board, allow the Board to access the information recorded on the computer system on which those records are held by means of the audit function referred to in clause 16.1.4(b) to the extent necessary for the Board to confirm that the audit function is enabled and functioning correctly.'

[58] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014

[59] Welcome to the Information Governance Toolkit (NHS), https://www.igt.hscic.gov.uk/ (lass access March 2014)

9.7.12.4) or electronically transferred outside the practice (Section 10.6.2.1.3 C). However, *The Guidance on the implementation of encryption within NHS Organisations*[60] says that encryption may be needed (for patient identifiable data) in some situations following a suitable risk assessment.

Hospitals in England are not mandated to have any specific EHR (IT) system. While there are preferred IT systems, a hospital can procure an IT system from anywhere subject to them meeting various requirements (functionality, security etc.). The approval process for any EHR system will involve a long process where a business case needs to be made and various issues such as funding, risk, governance, benefits and stakeholder needs (e.g. a plastic surgeon may need a system that can process images) are considered. Implementation of the system will involve many processes such as staff training, and transferring live existing paper records into the new electronic system.[61]

[60] The Guidance on the implementation of encryption within NHS Organisations, http://systems.hscic.gov.uk/infogov/security/infrasec/iststatements/dataenc_html (last access February 2014)
[61] Interview with East and North Hertfordshire NHS Trust on 21st March 2014

### 2.2.2. Table on requirements on the institutions hosting EHRs data

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Are there specific national rules about the hosting and management of data from EHRs?* | The Good Practice Guidelines for GP electronic patient records - version 4 (2011)[62] | SCRs are uploaded from GPs surgeries onto a central database managed by the Department of Health.<br><br>There are, however, national regulations in England that pertain to the creation, hosting and management of computerised medical records for any person who contracts to supply health care services for the NHS as give in *The National Health Service (General Medical Services Contracts) Regulations 2004* as amended and the *Good Practice Guidelines for GP electronic patient records - version 4 (2011).* |
| *Is there a need for a specific authorisation or licence to host and process data from EHRs?* | Health and Social Care Act 2012[63] | England (medical records held by contractors with the NHS)<br><br>Under the *Health and Social Care Act 2012*. Chapter 3, clause 81(1) 'Any person who provides a health care service for the purposes of the NHS must hold a licence under this Chapter.'<br>Clause 83 however, states that regulations may grant exemptions from clause 81 for (i) a prescribed person or health care service or (ii) persons or health care services of a prescribed description. |
| | The National Health Service (General Medical Services Contracts) Regulations 2004 as amended (Section 73) | *The Standard General Medical Services Contract – April 2012*, is required to be signed by a Contractor providing medical services to the NHS (The NHS Commissioning Board) and contains provisions for keeping computerised records. It reflects requirements of *The National Health Service (General Medical Services Contracts) Regulations 2004 (Section 73). The Standard General Medical Services Contract – April 2012* is quoted below because it contains updates to the original 2004 legislation with regard to the standards for GP computerised equipment and the Good Practice Guidelines for General Practice Electronic Patient Records |

[62] The Good Practice Guidelines for GP electronic patient records - version 4 (2011) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215680/dh_125350.pdf (last access February 2014)
[63] Health and Social Care Act 2012, http://www.legislation.gov.uk/ukpga/2012/7/pdfs/ukpga_20120007_en.pdf (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | The Standard General Medical Services Contract – April 2012[64] | Version 4, 2011.<br><br>*The Standard General Medical Services Contract – April 2012* clause 16.1.2. states that:<br>'The Contractor shall keep adequate records of its attendance on and treatment of its patients and shall do so-<br>(a) on forms supplied to it for the purpose by the Board; or<br>(b) with the written consent of the Board, by way of computerised records, or in a combination of those two ways' |
| *Are there specific obligations that apply to institutions hosting and managing data from EHRs (e.g. capacity, qualified staff, or technical tools/policies on security confidentiality)?* | The Standard General Medical Services Contract – April 2012 | *The Standard General Medical Services Contract – April 2012, clause 16.1.4* contains specific requirements for the computer system used to store EHRs (General Practice Systems of Choice Level 2 (GPSoC)[65]) and also an obligation to abide by guidelines contained in the *Good Practice Guidelines for General Practice Electronic Patient Records (version 4)*.<br><br>Clause 16.1.4 states:<br>'The consent of the Board required by clause 16.1.2(b) shall not be withheld or, once given, withdrawn provided the Board is satisfied, and continues to be satisfied, that-<br>(a) the computer system upon which the Contractor proposes to keep the records has been accredited by the Secretary of State or another person on his behalf in accordance with General Practice Systems of Choice Level 2;<br>(b) the security measures, audit and system management functions incorporated into the computer system as accredited in accordance with sub-clause (a) have been enabled; and<br>(c) the Contractor is aware of, and has signed an undertaking that it will have regard to the guidelines contained in "Good Practice Guidelines for General Practice Electronic Patient Records (version 4)" published on 21st March 2011...' |

[64] The Standard General Medical Services Contract – April 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/184931/Standard_General_Medical_Services_Model_Contract.pdf (last access February 2014)

[65] GPSoC provides practices with a choice of systems from GPSoC Framework suppliers, alongside choices offered by their Local Service Provider (LSP), in line with the requirements of the GMS contractual agreement. see GPSoc Overview, HSCIS, http://systems.hscic.gov.uk/gpsoc/summary/overview (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | With regard to staff, clause 16.2.1. states that 'The Contractor shall nominate a person with responsibility for practices and procedures relating to the confidentiality of personal data held by it.'<br><br>Staff must also under go SCR concept training. Any organisation having access to the SCR must have a Privacy officer in place (see clause 16.2.1 above). This Privacy Officer must be trained to interrogate the technical systems to investigate any allegations of inappropriate access to records.<br><br>There is an Information Governance toolkit against which organisations have to self declare and there are specific controls in there for the use of electronic information by health and social care organisations[66]. All organisations must assess themselves against requirements for : Management structures and responsibilities (e.g. assigning responsibility for carrying out the information governance assessment, providing staff training); Confidentiality and data protection; and Information security |
| | *The National Health Service (General Medical Services Contracts) Regulations 2004* | *The National Health Service (General Medical Services Contracts) Regulations 2004* as amended (Schedule 6, Section 74A (1)) states that 'A contractor must use the facility known as "GP2GP" for the safe and effective transfer of any patient records..'<br><br>Hospitals in England are not mandated to have any specific EHR system. While there are preferred IT systems, a hospital can procure an IT system from anywhere subject to them meeting various requirements (functionality, security etc.). The approval process for any EHR system will involve a long process where a business case needs to be made and various issues such as funding, risk, governance, benefits and stakeholder needs (e.g. a plastic surgeon may need a system that can process images) are considered. Implementation of the system will involving many processes such as the need for staff training, and transferring live existing paper records into the new electronic system.[67] |

[66] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014
[67] Interview with East and North Hertfordshire NHS Trust on 21st March 2014

| Questions | Legal reference | Detailed description |
|---|---|---|
| *In particular, is there any obligation to have the information included in EHRs encrypted?* | The Good Practice Guidelines for GP electronic patient records - version 4 (2011) | The Guidance on the implementation of encryption within NHS Organisations[68] says that encryption may be needed (for patient identifiable data) in some situations following a suitable risk assessment.<br><br>*The Good Practice Guidelines for GP electronic patient records - version 4 (2011)* requires encryption where electronic data is removed from GP practice premises (Section 9.7.12.4) or electronically transferred outside the practice (Section 10.6.2.1.3 C) |
| *Are there any specific auditing requirements for institutions hosting and processing EHRs?* | The Standard General Medical Services Contract – April 2012 | *The Standard General Medical Services Contract – April 2012*, clause 16.1.4 (b) mandates that the auditing functions of the computerised system must be enabled.<br><br>Also clause 16.1.5. states:<br>'Where a patient's records are computerised records, the Contractor must, as soon as possible following a request from the Board, allow the Board to access the information recorded on the computer system on which those records are held by means of the audit function referred to in clause 16.1.4(b) to the extent necessary for the Board to confirm that the audit function is enabled and functioning correctly.' |

[68] The Guidance on the implementation of encryption within NHS Organisations, http://systems.hscic.gov.uk/infogov/security/infrasec/iststatements/dataenc_html (last access February 2014)

## 2.3. Patient consent

### 2.3.1. Main findings

*GP and Hospital EHRs*
With regard to GP and hospital records, the NHS (England) has the legal authority to create patient records (in paper or computerised format) without the express or implied consent of a patient.[69] A patient cannot prevent the creation of a medical record either in paper or electronic form.

The increase in multi-disciplinary care in the GP and community settings, have led to a demand for sharing of patient records. GP records are now implemented on IT systems (e.g. TPP SystmOne) that facilitate the sharing of patient record across care providers[70]. Such records are called Shared Electronic Patient Records (SEPR). Sharing is governed by the Data Protection Act 1998. Data can be shared for healthcare purposes subject to the data protection principles, however, the Data Protection Act 1998 prevents the sharing of EHRs for non-healthcare purposes without patient's explicit consent.

*The Confidentiality and Disclosure of Information (General Medical Services, Personal Medical Services and Alternative Provider Medical Services) Directions 2013* addresses the legal framework for sharing.

> Direction 9: 'Information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, or some other legal basis, such as a robust public interest or legal justification for doing it'.
>
> Direct 10:'Generally patients who present for care are assumed to consent to the required information sharing between clinicians for the purpose of their individual healthcare needs, and those in the NHS to whom they are accountable.'

In 2009 the Royal College of General Practitioners published its Shared Record Professional Guidance (SRPG) report[71] relating to Shared Electronic Patient Record (SEPR)[72] systems and organisational/local Detailed Care Records (DCRs)[73]. The report resulted in 16 principles reflecting requirements under data protection legislation and other best practices. Principles 14 and 15 of the report directly address the issue of patient consent for sharing :

> 'Principle 14. Health organisations should be able to explain to patients who will have access to their SEPR/sDCR and must make information available to patients about such disclosures.
>
> Principle 15.
> Health professionals should respect the wishes of those patients who object to particular information being shared with others providing care through a SEPR/sDCR system, except where disclosure is in the public interest or a legal requirement.'.

Under the Health and Social Care Act 2012, the HSCIC is empowered to collect medical information from GP practices for secondary uses. Patients have a right to object to any personal confidential data

[69] The National Health Service (General Medical Services Contracts) Regulations 2004 as amended (Section 73(2))
[70] Your electronic patient record and the sharing of information: A patient's guide. http://www.tpp-uk.com/wp-content/uploads/2013/10/Enhanced-DSM-3.01-model-A-guide-for-patients.pdf (last access February 2014)
[71] Informing shared clinical care: Final report of the Shared Record Professional Guidance project, June 2009. RCGP. http://www.rcgp.org.uk/Clinical-and-research/Practice-management-resources/~/media/Files/Informatics/Health-Informatics-SRPG-final-report.ashx (last access February 2014)
[72] The Shared Electronic Patient Record (SEPR) is a generic term to encompass all forms of electronic patient records.
[73] The organisational/local Detailed Care Record (DCR) is a record containing everything relevant to the care of a patient that is known by the organisation..

being extracted unless there is a statutory duty to share information, a court order or an overriding public interest in disclosure.

Under the *NHS Act 2006 (Section 251)* the Secretary of State can make regulations to override the common law duty of confidentiality to enable the disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent is not practical, having regard to the cost and technology available.

The Caldicott 2 review panel (which reviewed the information governance framework in NHS organisations) reached a number of conclusions regarding consent and the sharing of patient data including the following[74] :

- '..across the health and social care system, implied consent is only applicable in instances of direct care.' (p, 37),
- '..only relevant information about a patient should be shared between professionals in support of their care.' (p, 37).
- '..consent should be obtained before sharing a patient's whole care record with other registered and regulated health and social care professionals for the purposes of direct care. Any exceptions to this guidance should be based on professional judgement in individual cases.' (p, 38).
- '..ways should be found to enhance patients' awareness of how their personal confidential data is used and strengthen staff understanding of the scope and limitations of implied consent.' (p.57).

*National Summary EHRs*

In England, all patients (aged 16 and over) are sent an information pack on the creation of a Summary Care Record (SCR) from their GP practice (at least twelve weeks before an SCR is created)[75]. They are informed that an SCR will be created automatically unless they choose to opt-out by completing and signing a special form sent to them or available online. They can seek further advice via various signposted information sources. If they wish to have an SCR they are not required to take any action and one will be created for them. If they do not wish to have an SCR they are required to complete the opt-out form and return it to their GP practice.

The opt-out form gives patient the following information on what it means not to have an SCR: 'NHS healthcare staff caring for you may not be aware of your current medications, allergies you suffer from and any bad reactions to medicines you have had, in order to treat you safely in an emergency. Your records will stay as they are now with information being shared by letter, email, fax or phone.'[76]

When an SCR is first created, details of the patient's medications, adverse reactions and allergies will be copied from the patient record of his GP into the SCR under "informed implied consent"[77]. More information can be added subject to the "explicit consent" of the patient[78].

Children get an SCR but are not informed about an SCR. A child or a parent (on behalf of a child where the child lacks Gillick competence) may make an opt-out request. Under specific circumstances where a GP feels that the best interests of the child warrant the creation of an SCR, the opt-out request will not be processed.

---

[74] Information: To share or not to share? The Information Governance Review, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf (last access March 2014)

[75] Powell, T & Thompson, G (2010), Electronic Patient Records: the roll-out of the Summary Care Record (House of Commons Library) p.9, http://www.parliament.uk/briefing-papers/sn05601.pd (last access February 2014)

[76] ibid

[77] Clay, R (2011) Summary Care Record Scope, NHS Connecting for Health. http://www.connectingforhealth.nhs.uk/systemsandservices/scr/documents/scrscope.pdf (last access February 2014)

[78] Ibid

An SCR on a GP IT system is created with four consent preferences[79]:

- Implied consent for medication, allergies, and adverse reactions only.
- Express consent for medication, allergies, and adverse reactions only
- Express consent for medication, allergies, adverse reactions AND additional information
- Express dissent (opted out) – Patient does not want an SCR

Where a patient has not completed an opt-out form, the default setting in the GP IT system will be implied consent. After creation of an SCR a patient can change his preferences at any time (but can no longer return to the implied consent preference). A patient can change his preference by giving express consent (by completing a form) to have additional information added to the core of his/her SCR. A patient can decide to opt-out after an SCR has been created. A patient can revert to a core SCR by giving express consent for a core SCR only or one with addition information. These changes are recorded via consent management screens on the GP IT system.

SCRs are held on a central computer and can be viewed/accessed nationally by healthcare staff directly involved in the care of a patient. A patient's consent is needed each time an SCR needs to be viewed/accessed (by a healthcare professional or a group of healthcare staff). If the patient is unable to consent at the specific time (e.g. due to being unconscious) and it is in the best interests of the patient to view their SCR then the SCR will be accessed without the patient's permission, but this access will be noted on the patient's SCR.

SCRs are not shared across borders. Also the different national health systems in the UK do not share their summary records.

[79] NHS, Introduction of New Summary Care Records Consent Codes, http://systems.hscic.gov.uk/scr/documents/consentcodes.pdf

### 2.3.2. Table on patient consent

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Are there specific national rules on consent from the patient to set-up EHRs?* | The National Health Service (General Medical Services Contracts) Regulations 2004 (Section 73) as amended | *The Standard General Medical Services Contract – April 2012* clause 16.1.2. states that:<br>'The Contractor shall keep adequate records of its attendance on and treatment of its patients and shall do so-<br>(a) on forms supplied to it for the purpose by the Board; or<br>(b) with the written consent of the Board, by way of computerised records, or in a combination of those two ways' |
| | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012) | SCRs<br>An SCR is created with the (implicit) consent of a patient.<br>All patients (16 years and over) are sent information packs containing a letter from their Primary Care Trust,[81] a Patient Summary leaflet and a Freepost op-out form. Patients are given a period of time (about 12 weeks) to decide whether they wish to have an SCR created for them. They can seek further advice via various signposted information sources. If they wish to have an SCR they are not required to take any action and one will be created for them. If they do not wish to have an SCR they are required to complete the opt-out form and return it to their GP practice.<br><br>Note: Children get an SCR but are not informed about an SCR. A child or a parent (on behalf of a child where the child lacks Gillick competence) may make an opt-out request. Under specific circumstances where a GP feels that the best interests of the child warrant the creation of an SCR, the opt-out request will not be processed.<br><br>An SCR on a GP IT system is created with four consent preferences[82]:<br>• Implied consent for medication, allergies, and adverse reactions only.<br>• Express consent for medication, allergies, and adverse reactions only |

[81] Primary Health Care Trusts were abolished by the Health and Social Care Act 2012, they were replaced by Clinical commissioning groups (CCGs)

[82] NHS, Introduction of New Summary Care Records Consent Codes, http://systems.hscic.gov.uk/scr/documents/consentcodes.pdf

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | • Express consent for medication, allergies, adverse reactions AND additional information<br>• Express dissent (opted out) – Patient does not want an SCR<br><br>Where a patient has not completed an opt-out form, the default setting in the GP IT system will be implied consent. After creation of an SCR a patient can change his preferences at any time (but can no longer return to the implied consent preference). A patient can change his preference by giving express consent to have additional information added to the core of his SCR. A patient can decide to opt-out after an SCR has been created. A patient can revert to a core SCR by giving express consent for a core SCR only or one with addition information. These changes are recorded via consent management screens on the GP IT system.<br><br>GP and hospital EHRs<br>With regard to GP and hospital records, the NHS has the legal authority to create patient records (in written or computerised format) without the express or implied consent of a patient. The patient also cannot prevent the creation of an electronic health record. |
| | The National Health Service (General Medical Services Contracts) Regulations 2004 (Section 73(2)) as amended[80] | *The National Health Service (General Medical Services Contracts) Regulations 2004 (Section 73(2))* as amended states that:<br>'The contractor shall keep adequate records of its attendance on and treatment of its patients and shall do so—<br>(a) on forms supplied to it for the purpose by the [the Board]; or<br>(b) with the written consent of the [the Board], by way of computerised records, or in a combination of those two ways.'<br><br>*Scotland*<br>Like the SCR (England), the ECS in Scotland is created using an implicit consent model. Patients can inform their GPs if they do not want an ECS. |

[80] The National Health Service (General Medical Services Contracts) Regulations 2004, http://www.legislation.gov.uk/uksi/2004/627/pdfs/uksi_20040627_en.pdf.
This most recent amendments to this act was made byThe National Health Service (Primary Medical Services) (Miscellaneous Amendments and Transitional Provisions) Regulations 2013, http://www.legislation.gov.uk/uksi/2013/363/contents/made (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | For the ePCS[83], explicit consent will be taken by GP from patient prior to sending the ePCS extract due to larger/more sensitive dataset than ECS. If the patient does not give consent or the Consent Tick-box is not completed the patient's data will not be uploaded to the ECS store & will not be viewable by NHS24/OOH Services. |
| *Is a materialised consent needed?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012) | After receiving notification regarding creation of an SCR, if patients wish to have an SCR they are not required to take any action and one will be created for them.<br><br>If a patient wishes to change their decision about their SCR after it has been created then express consent must be given by the patient (or by someone on behalf of the patient) by filling out a form provided by the GP's surgery. |
| *Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?* | | Patients are sent information about purposes of an SCR and also directed to additional sources of information about the SCR. They are also sent an opt-out form[84] if they do not want an SCR created.<br><br>The opt-out form gives patient the following information on what it means not to have an SCR: 'NHS healthcare staff caring for you may not be aware of your current medications, allergies you suffer from and any bad reactions to medicines you have had, in order to treat you safely in an emergency. Your records will stay as they are now with information being shared by letter, email, fax or phone.'[85] |
| *Are there specific national rules on consent from the patient to share* | The Good Practice Guidelines for GP | Multidisciplinary care in the GP and community have led the need for sharing patient records across different care setting. Such records are |

[83] Electronic Palliative Care Record http://www.scotshi.bcs.org.uk/hs09/Day2_Carrington_PeterKiehlmann_ePalliativeCareRecord.pdf (last access February 2014)
[84] SCR opt-out form, http://www.nhscarerecords.nhs.uk/optout/optout.pdf
[85] ibid

| Questions | Legal reference | Detailed description |
|---|---|---|
| *data?* | electronic patient records - version 4 (2011)- Chapter 5. | usually termed - Shared Electronic Patient Records (SEPR).<br><br>Sharing is governed by the Data Protection Act 1998 - Data can be shared for healthcare purposes subject to the data protection principles, however, the Data Protection Act 1998 prevents the sharing of EHRs for non-healthcare purposes without a patients explicit consent. |
| | Informing shared clinical care: Final report of the Shared Record Professional Guidance project, June 2009. RCGP. | In 2009 the Royal College of General Practitioners published its Shared Record Professional Guidance (SRPG) report. The report produced 16 principles that reinforce the principles of data protection legislation and other legal requirements. Principles 14 and 15 directly address consent from patients.<br><br>'Principle 14.<br>Health organisations should be able to explain to patients who will have access to their SEPR and must make information available to patients about such disclosures.<br>Principle 15.<br>Health professionals should respect the wishes of those patients who object to particular information being shared with others providing care through a SEPR system, except where disclosure is in the public interest or a legal requirement.' |
| | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012) | SCRs are held on a central computer and can be viewed/accessed nationally by healthcare staff directly involved in the care of a patient. A patient's consent is needed each time an SCR needs to be viewed/accessed (by a healthcare professional or a group of healthcare staff). If the patient is unable to consent at the specific time (e.g. due to being unconscious) and it is in the best interests of the patient to view their SCR then the SCR will be accessed without the patient's permission, but this access will be noted on the patient's SCR. |
| | The Confidentiality and | |

| Questions | Legal reference | Detailed description |
|---|---|---|
| | Disclosure of Information (General Medical Services, Personal Medical Services and Alternative Provider Medical Services) Directions 2013[86] | Provisions for other EHRs (GP surgeries and Hospitals) are governed by the Data Protection Act 1998 and are reflected in *The Confidentiality and Disclosure of Information (General Medical Services, Personal Medical Services and Alternative Provider Medical Services) Directions 2013*.<br><br>Direction 9 states that 'Information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, or some other legal basis, such as a robust public interest or legal justification for doing it'.<br><br>Direct 10 states that 'Generally patients who present for care are assumed to consent to the required information sharing between clinicians for the purpose of their individual healthcare needs, and those in the NHS to whom they are accountable.' |
| | Under the NHS Act 2006 (Section 251) [87] | *Under the NHS Act 2006 (Section 251)* the Secretary of State can make regulations to override the common law duty of confidentiality to enable the disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent is not practical, having regard to the cost and technology available. |
| | Information: To share or not to share? The Information Governance Review[88] (Caldicott 2 review) | The Caldicott 2 review panel (which reviewed the information governance framework in NHS organisations) reached a number of conclusions regarding consent and the sharing of patient data including the following:<br>- '..across the health and social care system, implied consent is only applicable in instances of direct care.' (p, 37)<br>- '..only relevant information about a patient should be shared between professionals in support of their care.' (p, 37)<br>- '..consent should be obtained before sharing a patient's whole care |

[86] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/183372/The_Confidentiality_and_Disclosure_of_Information_Directions_2013.pdf (last access February 2014)
[87] National Health Service Act (Section 251), http://www.legislation.gov.uk/ukpga/2006/41/section/251 (last access February 2014)
[88] Information: To share or not to share? The Information Governance Review, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf (last access March 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | record with other registered and regulated health and social care professionals for the purposes of direct care. Any exceptions to this guidance should be based on professional judgement in individual cases.' (p, 38) |
| *Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?* | | There are no opt-in/opt-out for patient consent with regard to processing SCRs, except that a patient can decide to opt-out of having an SCR at any time OR withhold consent to view an SCR. |
| *Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?* | | There are no opt-in/opt-out for patient consent with regard to sharing SCRs, except that a patient can withhold permission to view an SCR. |
| *Are there requirements to inform the patient about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012) | Patients are informed about the purposes of an SCR before they are created. Patients are informed about the consequences of opting out of creating an SCR when they complete an opt-out form. |
| *Can the patient consent to his/her EHRs being accessed by a health practitioner or health institution outside of the Member State (cross-border situations)?* | | Only healthcare staff directly involved in supporting or providing care for a patient can view a patient's SCR. Further an NHS smartcard and chip and passcode is needed to gain access. This means that cross-border sharing is not presently an option. |
| *Are there specific rules on patient consent to share data on a cross-border situation?* | | SCRs are not shared across borders. The different national systems in the UK do not share their summary records. |

## 2.4. Creation, access to and update of EHRs

### 2.4.1. Main findings

In England, GP and hospital medical records must be created for every patient seen or treated by a health care professioal. There is no stipulaton that medical records should be in electronic form. GP EHRs are accessed and updated by GPs and other authorised persons working in a GP practice (nurses, healthcare assistants, administration staff). Access to view certain fields within the GP EHR can be restricted by the use of smartcards and their associated role based access control roles. The implementation of this functionality, however, currently varies from one GP IT system to another. A system administrator can decide what access to grant to an individual based upon their individual job role. Any update entry will be date and time stamped as an entry by a particular individual within the GP IT record[89]. In hospitals a patient's medical record (whether in paper or electronic form) can be accessed by medical staff directly involved in the patient's care.[90]

With regard to SCRs, a patient is first informed about the creation of an SCR, and provided that he/she does not opt-out, the SCR is automatically created. The SCR is created with only three categories of data namely: a patient's medications, adverse reactions and allergies, taken from the patient's health record held by his/her General Practice[91]. Additional data can be added later, subject to explicit consent from the patient. Health care staff directly involved in a patient's care can access (via a smartcard and passcode) the patient's SCR after first obtaining permission from the patient. Access is limited to information required according to the role of the healthcare staff and is audited.

The SCR is held on a central computer (in pdf format) and only an organisation with a connection to the NHS N3 network[92] can access an SCR. This connection is obtained by applying to the HSCIC. An SCR can be accessed by healthcare staff providing or supporting a patient's care, i.e. healthcare staff who have a legitimate patient relationship. Access must be via an NHS Smartcard – it contains a chip and passcode, and facilitates role based access controls[93]. Before an NHS Smartcard is issued appropriate ID checks are made. Any access to an SCR will be audited – details of who accessed the SCR and any changes made to the SCR are recorded. All organisations must have a privacy officer and he must be trained to interrogate the technical systems to investigate any allegations of inappropriate access to records. Healthcare staff need to ask a patient's permission each time they want to access an SCR. Where it is not possible to seek permission from a patient (e.g. where the patient is unconscious), healthcare staff will access the SCR but will record this fact on the SCR.[94] Previously patients were able to access and view their SCR via the HealthSpace website owned by the National Health Service but this facility was recently shut down. At the present time (2014) patients can request a printed copy of their SCR from their GP practice[95]. Patients cannot change information written by healthcare staff but can request the correction of errors, The Department of Health have announced that from 2015 patients will be able to access their SCRs online[96].

The SCR is only updated in the GP practice IT system by an authorised user (GP, nurse, health care assistant, administration staff).

---

[89] Interview with SCR Primary Care Clinical Lead (HSCIC) on 8th April 2014.
[90] Information: To share or not to share? The Information Governance Review, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf (last access March 2014)
[91] Clay, R (2011) 'Summary Care Record Scope, NHS Connecting for Health', available at http://www.connectingforhealth.nhs.uk/systemsandservices/scr/documents/scrscope.pdf ((last access February 2014)
[92] **N3** is the national broadband network for the English National Health Service (NHS), connecting all NHS locations and 1.3 million employees across England.
[93] This is not the case in Scotland. They only use a username and password for access to their ECR. Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014
[94] Clay, R (2011) Summary Care Record Scope, NHS Connecting for Health. http://www.connectingforhealth.nhs.uk/systemsandservices/scr/documents/scrscope.pdf (last access February 2014)
[95] http://www.nhscarerecords.nhs.uk/faqs
[96] http://informationstrategy.dh.gov.uk/when-will-i-have-access/ (last access February 2014)

All SCR data are safeguarded by appropriate security measures. The SCR also adheres to the NHS Care Record Guarantee for England[97] which details collection, storage and access policies for patient records

There are no measures that consider access to the SCR by health professionals from another Member State. An NHS Smartcard and passcode is needed to access an SCR and this is only issued to NHS staff in England.

[97] NHS Care Record Guarantee, http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf (last access February 2014)

### 2.4.2. Table on creation, access to and update of EHRs

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Are there any specific national rules regarding who can create and where can EHRs be created?* | The National Health Service (General Medical Services Contracts) Regulations 2004 as amended (Section 73(2)) | *The National Health Service (General Medical Services Contracts) Regulations 2004 (Section 73(2))* as amended empowers NHS 'contractors' (GP surgeries and health service providers) to create a medical record (although an EHR is not specified). See Table 2.3.2 above<br><br>An SCR is created at a patient's GPs surgery from information in a patient's detailed EHR. |
| *Are there specific national rules on access and update to EHRs?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 7. | GP EHRs are accessed and updated by GPs and other authorised persons working in a GP practice (nurses, healthcare assistants, administration staff). Patient consent is implicit. Any update entry will be date and time stamped as an entry by a particular individual within the local GP IT record[98].<br><br>In hospitals a patient's medical record (whether in paper or electronic form) can be accessed by medical staff directly involved in the patient's care.[99]<br><br>A patient's consent is needed each time an SCR needs to be viewed/accessed (by a healthcare professional or a group of healthcare staff). If the patient is unable to consent at the specific time (e.g. due to being unconscious) and it is in the best interests of the patient to view their SCR then the SCR will be accessed without the patient's permission, but this access will be noted on the patient's SCR. Users of SCRs do not have access to the GP source detailed EHR.<br><br>The SCR is held on a central computer and only an organisation with a connection to the N3 network can access an SCR. This connection is |

[98] Interview with SCR Primary Care Clinical Lead (HSCIC) on 8th April 2014.
[99] Information: To share or not to share? The Information Governance Review, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf (last access March 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | obtained by applying to the HSCIC. All organisations must have a privacy officer and he must be trained to interrogate the technical systems to investigate any allegations of inappropriate access to records[100].<br><br>There is need for a registration authority to issue smartcards to individual people to enable access to an SCR. These smartcards will have role-based access control built into them[101]. |
| *Are there different categories of access for different health professionals?* | | GP EHRs are held locally in a GP practice and are accessed by the GP and other authorised persons working in the GP practice. Access to view certain fields within the patient record can be restricted by the use of smartcards and their associated role based access control roles. The implementation of this functionality, however, currently varies from one GP IT system to another - so the answer to this question could be yes or no depending on the particular clinical system used by the practice A system administrator can decide what access to grant to an individual based upon their individual job role. However, some practices will take a view to grant greater access (for a given individual) to the EMR 'just in case' the functionality would be needed. Also, most GP IT systems will allow access to the EMR through a login and password only, without inserting the smartcard - so these restrictions can be bypassed in practice.[102]<br><br>Some IT systems enable sharing of health data among different clinical care settings (e.g. GP, District nures and smoking clinic).[103] |
| | The NHS Summary Care Record | Role Based Access Control is implemented for SCRs. This controls |

[100] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014
[101] ibid.
[102] Interview with SCR Primary Care Clinical Lead (HSCIC) on 8th April 2014.
[103] For example see: Your electronic patient record and the sharing of information: A patient's guide. http://www.tpp-uk.com/wp-content/uploads/2013/10/Enhanced-DSM-3.01-model-A-guide-for-patients.pdf (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | Guide for GP Practice Staff V1.2 (October 2012), page 25. | what information a particular user is allowed to access. For example certain users may be restricted to viewing only demographic information compared to clinical information. |
| *Are patients entitled to access their EHRs?* | Data Protection Act 1988 (Part II, Section 7).<br><br>The NHS Constitution (for England 26th March 2013)[104]<br><br>1.1.1 The Data Protection (Subject Access Modification)(Health) Order 2000<br><br>The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 25. | As part of the Subject Request provisions of the *Data Protection Act 1988 (Part II, Section 7)*, patients are entitled to access their EHRs. *The NHS Constitution (for England 26th March 2013) Section 3a*, page 8 also states: 'You have the right of access to your own health records and to have any factual inaccuracies corrected.'<br><br>*The Data Protection (Subject Access Modification)(Health) Order 2000* amended the Data Protection Act 1998 by stipulating that information need not be disclosed if it would be likely to cause serious harm to the physical or mental health of the data subject or any other person.<br><br>Patents can ask to see a copy of their SCR or GP EHR or hospital records. At the time of writing patients cannot access their SCR or GP EHR online. |
| *Can patient have access to all of EHR content?* | The Data Protection (Subject Access Modification)(Health) Order 2000<br><br>The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 25 | As noted above, *The Data Protection (Subject Access Modification)(Health) Order 2000* amended the Data Protection Act 1998 by stipulating that information need not be disclosed if it would be likely to cause serious harm to the physical or mental health of the data subject or any other person. Hence a patient may not always have access to all of his EHR.<br><br>The copy of the content of an SCR given to a patient will contain all the contents of the SCR |
| *Can patient download all or some of EHR content?* | A mandate from the Government to the NHS Commissioning Board: April 2013 to March | At the time of writing patients cannot access their SCR online. However by 2015 the NHS Commissioning Board (NHS CB) expects all general practices in England to offer patients online viewing access |

[104] The NHS Constitution (for England 26th March 2013), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170656/NHS_Constitution.pdf (last access February 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | 2015 (November 2013)[105] | to their medical records. |
| *Can patient update their record, modify and erase EHR content?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 25. | Patients can only view their GP EHR. They cannot modify or erase any content. However, if any inaccuracies are spotted then the patients can notify their GP surgery.<br><br>A patient cannot change information written in an SCR, however if they see errors or information in their SCR then they can inform their GP practice about it.[106] |
| *Do different types of health professionals have the same rights to update EHRs?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 4. | It is usual for all members of the GP practice team to be able to write to the EPR (including nurses, health care assistants and administration staff) - but that entry will be date and time stamped as an entry by a particular individual within the local GP IT record.[107]<br><br>The SCR is only updated in the GP practice IT system by an authorised user (GP, nurse, health care assistant, administration staff). That detail about the author of a particular data item, though included in the local GP IT record, would not be transferred to a summary such as the SCR. The SCR has a single author and is date and time stamped - but the author will be the person who triggered the sending of the SCR, rather than the person who last updated an individual data item within the local GP IT system record.[108] |
| *Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 25. | The SCR can only be accessed by authorised healthcare staff. |
| *Are there exceptions to the access requirements (e.g. in case of emergency)?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 7. | The SCR was created for emergency and after hours care. Consent form the patient is required every time an SCR needs to be viewed. If the patient is unable to consent at the specific time (e.g. due to being unconscious) and it is in the best interests of the patient to view their |

[105] A mandate from the Government to the NHS Commissioning Board: April 2013 to March 2015 (November 2013) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/256497/13-15_mandate.pdf (last access February 2014)
[106] NHS, SCR Frequently asked questions, http://www.nhscarerecords.nhs.uk/faqs (last access February 2014)
[107] Interview with SCR Primary Care Clinical Lead (HSCIC) on 8th April 2014
[108] ibid.

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | SCR then the SCR will be accessed without the patient's permission, but this access will be noted on the patient's SCR. |
| *Are there any specific rules on identification and authentication for health professionals?*<br>*Or are they aggregated?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 25. | In order to access an SCR, authorised healthcare staff must use an NHS Smartcard and a pass code. Before an NHS Smartcard is issued appropriate ID checks are made.<br><br>That is not the case in Scotland. They have not gone down that route. They have just gone for username and password. Which serves the same function as a two-factor authentication. England thought that smartcards were more secure[109]. |
| *Does the patient have the right to know who has accessed to his/her EHRs?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 26. | There is no right established, however, audit trails are created when an SCR is accessed. An alert will trigger automatically when there is suspected inappropriate access. |
| *Is there an obligation on health professionals to update EHRs?* | The Data Protection Act 1998, Schedule 1, Part 1 | Under the Data Protection Act 1988, Schedule 1, Part 1, the fourth data protection principle states that Personal data should be accurate and, where necessary, kept up to date'. |
| *Are there any provisions for accessing data on 'behalf of' and for request for second opinion?* | The NHS Summary Care Record Guide for GP Practice Staff V1.2 (October 2012), page 25. | To view a patient's SCR, healthcare staff must be involved in the patient's care, (i.e. there must be a legitimate relationship with the patient). |
| *Is there in place an identification code system for cross-border healthcare purpose?* | | There are no cross border provisions for using the SCR. |
| *Are there any measures that consider access to EHRs from health professionals in another Member State?* | | There are no measures that consider access to the SCR from health professionals from another Member State. An NHS Smartcard and pass code is needed to access an SCR and this is only issued to NHS staff in the specific NHS home country (e.g. England). |

[109] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.

## 2.5. Liability

### 2.5.1. Main findings

In England, The General Medical Council's (GMC) *Good Medical Practice (2013)* sets out the standards required for registered doctors. It mandates that a patient's condition needs to be adequately assessed taking into account their history. The latter will involve accessing an EHR (or other medical record where possible) before take a decision involving the patient.

*The Good Practice Guidelines for GP electronic patient records - Version 4 (2011)* Section 8b.6, accepts that EHR will contain errors. Page 118 states that 'However carefully electronic records are kept, errors in their content will sometimes be present.'

In the UK medical negligence is proved where: a physician owns the patient a duty of care; there is a breach of that duty (e.g. substandard practice); causation can be proved (i.e. the sub-standard practice led to harm); and the harm is not too remote. Establishing a breach of duty in healthcare is subject to the Bolem test (*Bolam v Friern Hospital Management Committee* (*1957) 1 WLR 583*) modified by the Bolitho amendment (*Bolitho v. City and Hackney Health Authority [1997] 4 All ER 771*). Under the Bolem test, a doctor does not breach the legal standard of care, and is therefore not negligent, if his actions conformed to a practice supported by a body of professional opinion. In the case of Bolitho a new requirement was imposed that the standard proclaimed must be justified on a logical basis and must have considered the risks and benefits of competing options.

In England, there is no specific legislation regarding medical negligence related to the use of EHRs per se. EHRs and paper records are treated equally in existing legislation.

Under the Data Protection Act 1988, Principle 7, data controllers must put in place adequate technical and organisational measures to safeguard personal data (which they are processing) from destruction, adequate loss, unauthorised access or disclosure.

Business continuity of EHR systems is a specific area of liability that needs to be carefully addressed. This means if there is a power failure or the EHR system fails to function properly then there would be no access to EHRs of patients and someone needs to take responsibility for managing such an eventuality. This would involve having a business continuity plan in place. The length of time that the system would be out of use and whether the system failure is catastrophic will need to be investigated. Methods should be in place to archive data on a regular basis to ensure that historical data is not lost and that data can be recovered in the event of a failure that results in data loss. Paper records may need to be in place to revert to.[110]

[110] Interview with East and North Hertfordshire NHS Trust (last access March 2014)

### 2.5.2. Table on liability

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Does the national legislation set specific medical liability requirements related to the use of EHRs?* | | There is no national legislation on special liability regarding EHRs. |
| *Can patients be held liable for erasing key medical information in EHRs?* | | Patients are not able to change or erase information contained in their SCR or GP EHR. |
| *Can physicians be held liable because of input errors?* | The Good Practice Guidelines for GP electronic patient records - version 4 (2011)<br><br>Bolam v Friern Hospital Management Committee (1957) 1 WLR 583<br><br><br><br><br>Bolitho v. City and Hackney Health Authority [1997] 4 All ER 771 | The Department of health accepts that EHRs may have errors. *The Good Practice Guidelines for GP electronic patient records - Version 4 (2011)* Section 8b.6, page 118 states that 'However carefully electronic records are kept, errors in their content will sometimes be present.'<br><br>Depending on the type of error, it may be possible for a physician to be liable, subject to proving negligence.<br><br>Negligence is proved where: a physician owns the patient a duty of care; there is a breach of that duty (e.g. substandard practice); causation can be proved (i.e. the sub-standard practice led to harm); and the harm is not too remote.<br><br>Establishing a breach of duty in healthcare is subject to the Bolem test modified by the Bolitho amendment.<br><br>Under the Bolem test, a doctor does not breach the legal standard of care, and is therefore not negligent, if his actions conformed to a practice supported by a body of professional opinion. In the case of Bolitho a new requirement was imposed that the standard proclaimed must be justified on a logical basis and must have considered the risks and benefits of competing options. |
| *Can physicians be held liable because they have erased data from the EHRs?* | | See previous comments |
| *Are hosting institutions liable in case* | The Data Protection Act | Under the Data Protection Act 1988, Principle 7, data controllers must put |

| Questions | Legal reference | Detailed description |
|---|---|---|
| *of defect of their security/software systems?* | 1988, Principle 7 | in place adequate technical and organisational measures to safeguard personal data (which they are processing) from destruction, adequate loss, unauthorised access or disclosure. |
| *Are there measures in place to limit the liability risks for health professionals (e.g. guidelines, awareness-raising)?* | The Good Practice Guidelines for GP electronic patient records - Version 4 (2011)<br><br>The Information Commissioner's Office guidance | *The Good Practice Guidelines for GP electronic patient records - Version 4 (2011)* gives guidance regarding the development, deployment and use of GP IT systems.<br><br>The Information Commissioner's Office has a webpage and various types of information for the health care sector[111]. |
| *Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?* | The Data Protection Act 1998, Principle 7 | Under the Data Protection Act 1988, Principle 7, data controllers must put in place adequate technical and organisational measures to safeguard personal data (which they are processing) from destruction, adequate loss, unauthorised access or disclosure. |
| *Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?* | GMC Good Medical Practice, 2013[112]<br><br>The Royal College of General Practitioners Curriculum 2010, revised in April 2013, at page 8.[113] | In the General Medical Council's (GMC) *Good Medical Practice (2013)* which sets out the standards required for registered doctors, they advise at no 15 as follows:<br><br>'If you assess, diagnose or treat patients, you must:<br><br>(a) adequately assess the patient's conditions, taking account of their history (including the symptoms and psychological, spiritual, social and cultural factors), their views and values; where necessary, examine the patient…'<br><br>*The Royal College of General Practitioners Curriculum 2010*, revised in April 2013, at page 8, point 1.6 states that GPs should 'Effectively use patient records (electronic or paper) during the consultation to facilitate high-quality patient care'. |

[111] ICO guidance for the health care sector, http://ico.org.uk/for_organisations/sector_guides/health (last access February 2014)
[112] Good Medical Practice (2013), General Medical Council, http://www.gmc-uk.org/static/documents/content/GMP_2013.pdf_51447599.pdf (last access February 2014)
[113] http://www.gmc-uk.org/2_01_The_GP_consultation_in_practice_April_2013.pdf_52883401.pdf

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Are there liability rules related to the misuse of secondary use of health data?* | Data Protection Act 1998; Common law duty of Confidence. | Liability rules for misuse of identifiable health data (personal data) will fall under the Data Protection Act 1988 and the common law duty of confidence. |

## 2.6. Secondary uses and archiving durations

### 2.6.1. Main findings

*Secondary uses*
In England, The Health and Social Care Act 2012, Part 9, Chapter 2, established The Health and Social Care Information Centre (HSCIC), responsible for various functions including collecting and analysing national health and social care data (termed care.data[114]) from GP practices Information is not collected from SCRs since SCRs are created and updated in the GP Practice using detailed GP records and information sent to GPs from out-of-hours or emergency treatment.

The HSCIC has a Secondary Uses Service (SUS) that is the single, comprehensive repository for healthcare data in England which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services. Secondary use services include commissioning services, improving public health and developing national policy. The HSCIC is empowered to collect patient data from GP surgeries and health care providers. Patients have a right to object to any personal confidential data being extracted unless there is a statutory duty to share information, a court order or an overriding public interest in disclosure. Data collected can be patient identifiable, anonymised or pseudonymised as required[115].

Information collected includes: ethnicity and any data from the previous four months about referrals, prescriptions or health information such as diagnoses. These diagnoses relate to health conditions such as diabetes, heart disease, stroke, cancers (including bowel, breast, and cervical), chronic liver disease, chronic kidney disease, asthma, damage to the retina of the eye, high blood pressure and dementia.

Information not collected includes: codes that relate to sensitive information including HIV/AIDS, sexually transmitted infections, termination of pregnancy, IVF treatment, marital status, complaints, convictions, imprisonment, and abuse by others.

*Archiving durations*
The Data Protection Act 1998, Principle 5 states that: 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'.

The ICO states that their approach has always been for data controllers to justify any retention period. They contend that in practice this means that in some circumstances it may be that personal data can only be retained for a short period, in other situations indefinite retention can be justified. Retention needs to be assessed on a "case-by-case" basis.[116]

However, the *Good Practice Guidelines for GP Electronic Patient Records* - Version 4 (2011*)*, states that EHRs are needed especially to provide medico-legal evidence (e.g. to establish or refute allegations of negligence or poor performance) and should be retained indefinitely by a practice, as they are the sole source of forensic evidence.

[114] care.data (HSCIC), http://www.hscic.gov.uk/article/3525/Caredata (last access March 2014)
[115] NHS England has made a commitment that personal confidential data will not be shared unless there is a legal basis or an overriding public interest in disclosure. See: http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-guide.pdf (last access March 2014)
[116] Interview with ICO on 5th March 2014.

### 2.6.2. Table on secondary uses and archiving durations

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Are there specific national rules on the archiving durations of EHRs?* | The Data Protection Act 1998, Principle 5 | The Data Protection Act 1998, Principle 5: 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'. The ICO contends that their approach has been for data controllers to justify any retention period. In practice this means that in some circumstances it may be that personal data can only be retained for a short period. However in other situations indefinite retention can be justified. It is all "case-by-case".[118] |
| | Records Management NHS Code of Practice Part 2 (2nd Edition), 2009[117] | *The Records Management NHS Code of Practice Part 2 (2nd Edition), 2009*, sets out the minimum retention periods for various types of health records. On page 7 it states that: 'Records (whatever the media) may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years.' |
| | The Good Practice Guidelines for GP electronic patient records - Version 4 (2011) | *The Good Practice Guidelines for GP electronic patient records - Version 4 (2011)* states that: 'The retention of audit trails and patient records by a practice that is no longer caring for the individual concerned must be for appropriate and necessary purposes. In the absence of a lawful basis for retaining these records they should be physically deleted from systems. If there is a lawful basis for retaining records they should be protected by security measures that prevent them from being accessed inappropriately.'<br><br>The guide however, cited that medical records are needed especially to provide medico-legal evidence (e.g. to establish or refute allegations of negligence or poor performance). The guide therefore states that: 'It is therefore necessary that both the audit trail and the associated patient record be retained indefinitely by a practice, as they are the sole source of forensic evidence.' (page 49) |
| *Are there different archiving rules for* | Records Management | Different medical records have different minimum retention periods. The |

[117] Records Management NHS Code of Practice Part 2 (2nd Edition), 2009, http://systems.hscic.gov.uk/infogov/links/recordscop2.pdf (last access February 2014)
[118] Interview with the ICO on 5th March 2014.

| Questions | Legal reference | Detailed description |
|---|---|---|
| *different providers and institutions?* | NHS Code of Practice Part 2 (2nd Edition), 2009 | Records Management NHS Code of Practice details retention periods for Hospitals and GPs |
| *Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?* | Records Management NHS Code of Practice Part 2 (2nd Edition), 2009<br><br>The Good Practice Guidelines for GP electronic patient records - Version 4 (2011*)* | At the end of a retention period, data should be destroyed under confidential conditions.<br><br>Is the case of GP EHRs, The Good Practice Guidelines for GP electronic patient records - Version 4 (2011*)* says that*:* 'It is therefore necessary that both the audit trail and the associated patient record be retained indefinitely by a practice, as they are the sole source of forensic evidence.' (page 49) |
| *Are there any other rules about the use of data at the end of the archiving duration or in case of closure of the EHR?* | | None identified. |
| *Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?* | Health and Social Care Act 2012[119], Part 9, Chapter 2. | Health data can be used for non-clinical secondary uses, e.g. health care planning, commissioning of health services, research, education and training.<br><br>The Health and Social Care Act 2012, Part 9, Chapter 2, established The Health and Social Care Information Centre (HSCIC), responsible for various functions including collecting, analysing and national health and social care data (termed care.data). The HSCIC is empowered to collect medical data from GP surgeries and health care providers.<br><br>The HSCIC has a Secondary Uses Service (SUS) that is the single, comprehensive repository for healthcare data in England which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services. On its website it states that:<br><br>'When a patient or service user is treated or cared for, information is collected which supports their treatment. This information is also useful for many other purposes such as: |

[119]Health and Social Care Act 2012, http://www.legislation.gov.uk/ukpga/2012/7/pdfs/ukpga_20120007_en.pdf (last access February 2014).

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | • Healthcare planning<br>• Commissioning services<br>• Payment by Results<br>• Improving public health<br>• Developing national policy<br><br>SUS is a data warehouse containing this patient-level information. Data can be clear (patient identifiable), anonymised or pseudonymised as required for the user's needs. NHS providers and commissioners can use this data for 'secondary uses'; purposes other than primary clinical care.'[120]<br><br>The UK Data Protection Act 1998 considers medical research to be a legitimate healthcare purpose for processing sensitive personal data. Therefore the current data protection requirements are not a barrier to secondary uses of medical data.[121] |
| *Are there health data that cannot be used for secondary use?* | Health and Social Care Act 2012, Section 259 | Under The Health and Social Care Act 2012, Section 259, the HSCIC has the power to require and request the provision of any information which it considers necessary, from a health or social care body or from any person who provides health care services or social adult care in England.<br>Section 259 (1) reads (1)<br>"The Information Centre may—<br>(a) require any person mentioned in subsection (2) to provide it with any information which the Centre considers it necessary or expedient for the Centre to have for the purposes of any function it exercises by virtue of this Chapter, and<br>(b) request any other person to provide it with such information."<br>The HSCIC has however indicated the kinds of information that will be collected from GP records[122]. |

[120] Secondary Uses Service, http://www.hscic.gov.uk/sus (last access February 2014).
[121] Interview with ICO, 5th March 2014.
[122] HSCIC, What we will collect from GP records under care.data
http://www.hscic.gov.uk/article/3915/What-we-will-collect-from-GP-records-under-caredata (last access March 2014)

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | Information collected:<br>Ethnicity and any data from the previous four months about referrals, prescriptions or health information such as diagnoses. These diagnoses relate to health conditions such as diabetes, heart disease, stroke, cancers (including bowel, breast, and cervical), chronic liver disease, chronic kidney disease, asthma, damage to the retina of the eye, high blood pressure and dementia.<br><br>Information not collected:<br>Codes that relate to sensitive information including HIV/AIDS, sexually transmitted infections, termination of pregnancy, IVF treatment, marital status, complaints, convictions, imprisonment, and abuse by others. |
| *Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?* | | As mentioned earlier the HSCIC Secondary Uses Service (SUS) warehouse contains patient data that can be patient identifiable, anonymised or pseudonymised as required for the user's needs.<br><br>While the HSCIC is empowered to collect any information it has indicated that it will not collect codes that relate to sensitive information including HIV/AIDS, sexually transmitted infections, termination of pregnancy, IVF treatment, marital status, complaints, convictions, imprisonment, and abuse by others. |
| *Does the law say who will be entitled to use and access this data?* | The Health and Social Care Act 2012 | The HSCIC will determine use of data for secondary purposes. |
| *Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?* | Data Protection Act 1998 | Under the Data Protection Act 1998, a patient can withdraw consent to the processing of personal information for secondary care purposes. A withdrawal form can be downloaded from the HSCIS website[123]. |

[123] HSCIS - Withdrawal of consent to the processing of personal information for secondary care purposes, http://www.hscic.gov.uk/policyprocs (last access February 2014)

## 2.7. Requirements on interoperability of EHRs

### 2.7.1. Main findings

In England, there is no legal instrument mandating the development of interoperable EHRs, however, *The National Health Service (General Medical Services Contracts) Regulations 2004 (Section 73)* has specific requirements for the computer systems used by GPs. (i.e. General Practice Systems of Choice Level 2). Different GP surgeries can have different IT systems supplied by different approved commercial providers.

SCRs are held on a centralised database. All IT systems in GP surgeries are technically able to create SCRs that are standardised.

Hospitals in England are not mandated to have any specific EHR system. While there are preferred IT systems, a hospital can procure an IT system from anywhere subject to the system meeting various requirements (functionality, security etc.). This means that different hospitals may have completely different IT systems and this does not foster interoperability. [124]

There are no specific rules/standards on the interoperability of EHRs.

There are no legal provisions for the interoperability of EHRs in UK countries and in EU Member States.

One challenge for interoperability is that clinical information has to be very specific. There are specific sets of codes which map clinical information and which have very specific identities. Those code sets are not all the same in every country. There are even different codes in England. For instance England is trying to automate the inclusion of some clinical data using technologies and there are two code sets in use that are being mapped to. One is called READ code and the other SNOMED code. The difficulty with applying technology is that different countries with different users may have developed their own different coding systems.[125] As noted previously in 2011 the Information Standards Board for Health and Social Care approved the adoption of the SNOMED CT code in England[126]. By 2015 all NHS staff (or staff at any organisation who deliver care on behalf of the NHS) interacting with patients should use SNOMED CT to record and exchange coded clinical information.

In England there many commercial suppliers of IT systems for GP practice. Each one has developed their systems differently. When the SCR developers are trying to extract data from GP systems onto a national spine, they have to talk to each of the suppliers and try to get their product to conform to various requirements so that they product can conform the SCR requirements to enable data to be extracted in a uniform way. The presence of different suppliers and the need to talk to each supplier which involves giving them money is a complication. Also commercial suppliers will not do anything unless it helps their profits. The organisation run by HSCIC called GPSOC (GP System of Choice) provides financial incentives to the GP system suppliers to meet the central requirements of the record. [127]

[124] Interview with East and North Hertfordshire NHS Trust on 21st March 2014.
[125] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.
[126] Information Standards Notice – New Standards, ISB, 2011. Available at http://www.isb.nhs.uk/documents/isb-0034/amd-26-2006/isn.pdf (last access February 2014).
[127] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.

### 2.7.2. Table on interoperability of data requirements

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Are there obligations in the law to develop interoperability of EHRs?* | | There are no legal instruments mandating the development of interoperable EHRs, however, *The National Health Service (General Medical Services Contracts) Regulations 2004 (Section 73)* has specific requirements for the computer systems used by GPs. The most recent standard is reflected in the *The Standard General Medical Services Contract – April 2012, i.e.* General Practice Systems of Choice Level 2.<br><br>However different GP surgeries can have different IT systems supplied by different approved providers (under General Practice Systems of Choice Level 2).<br><br>Hospitals in England are not mandated to have any specific EHR system. While there are preferred IT systems, a hospital can procure an IT system from anywhere subject to them meeting various requirements (functionality, security etc.).[128]<br><br>One challenge for interoperability is that clinical information has to be very specific. There are specific sets of codes which map clinical information and which have very specific identities. Those code sets are not all the same in every country. There are even different codes in England. For instance England is trying to automate the inclusion of some clinical data using technologies and there are two code sets in use that are being mapped to. One is called READ code and the other SNOMED code. The difficulty with applying technology is that different countries with different users may have developed their own different coding systems.[129] As noted previously in 2011 the Information Standards Board for Health and Social Care approved the adoption of the SNOMED CT code in England<br><br>In the UK there many commercial suppliers of IT systems for GP practice. |

[128] Interview with East and North Hertforshire NHS Trust on 21st March 2014.
[129] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | Each one has developed their systems differently. When the SCR developers are trying to extract data from GP systems onto a national spine, they have to talk to each of the suppliers and try to get their product to conform to various requirements so that they product can conform the SCR requirements to enable data to be extracted in a uniform way. The presence of different suppliers and the need to talk to each supplier which involves giving them money is a complication. Also commercial suppliers will not do anything unless it helps their profits. The organisation run by HSCIC called GPSOC (GP System of Choice) provides financial incentives to the GP system suppliers to meet the central requirements of the record. [130] |
| *Are there any specific rules/standards on the interoperability of EHR?* | | There is no specific rules/standards on the interoperability of EHRs, however from 2015 all NHS staff (or staff at any organisation who deliver care on behalf of the NHS) interacting with patients should use SNOMED CT to record and exchange coded clinical information. |
| *Does the law consider or refer to interoperability issues with other Member States systems?* | | There is no legal provision for the interoperability with other Member States. |

[130] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.

## 2.8. Links between EHRs and ePrescriptions

### 2.8.1. Main findings

In England the EHR system and Electronic Prescription Service (EPS) are fully integrated. Both the EHR and ePrescription are part of one system. They share data and the ePrescription is linked to the EHR via a unique patient NHS number. The action of prescribing is just another event that gets added to the EHR along with other events like a test result being returned from a pathology lab or a referral being made to somewhere or a diagnosis being made as part of a consultation. They are all just different entities that would be within the database of the clinical system. Every prescription must contain certain information including: the identity of the patient; the identity of the prescriber ; and the details of the medication prescribed. The relevant information goes into an electronic message that is sent to the Electronic Prescription Service (EPS), and it is the EPS that makes that message available for dispensers to access.[131]

The Electronic Prescription Service 'allows the transmission of prescription messages and digitally-signed prescriptions from primary care prescribers, via a central network and server infrastructure, the Spine, from where they can be downloaded by dispensing contractors including community pharmacists, dispensing appliance contractors and dispensing doctors.' [132]

*The National Health Service (General Medical Services Contracts) Regulations 2004 (Schedule 6, paragraph 39A) as amended* authorises any NHS contractor (GP, hospital doctor etc.) to use the Electronic Prescription Service. Every patient must be registered with a GP and will be given an NHS number. All GPs and hospitals must create a medical record for a patient, however the law does not stipulate that it must be in electronic form. A GP treating a patient will have access to a patient's EHR or if one does not exist a paper medical record. Also in the case of an emergency or out-of-hours care a healthcare professional will have access to the patient's SCR (which can be accessed nationally).

The GMC's *Good practice in prescribing and managing medicines and devices* advises that prescribing drugs should be done 'only when you have adequate knowledge of the patient's health, and are satisfied that the drugs or treatment serve the patient's needs.' (paragraph 1a.) The guide makes clear that access to the patient's health records is necessary. However there is no specific mention of EHRs (although most GPs hold patient records in electronic form). It is technically possible for an ePrescription to be generated once the relevant information about the patient, the prescriber and the medication (usually generated using an EHR) is entered into a system.

Under certain conditions a healthcare professional can write prescriptions without access to a patient's medical records. In the *BMA's Prescribing in General Practice guide*, May 2013, mention is made of non-GP prescribers and their responsibility for checking interactions and taking a full drug history if they do not have access to the main clinical record. The guidelines do not make any specific mention of ePrescriptions or EHRs.

[131] Interview with the EPS (HSCIC) on 6th March 2014

[132] The Evaluation Of The Electronic Prescription Service In Primary Care: Interim Report on the Findings from the Evaluation in Early Implementer Sites *9th. July, 2012*, page 3, available at: http://www.ucl.ac.uk/pharmacy/documents/staff_docs/EPS (last access February 2014)

### 2.8.2. Table on the links between EHRs and ePrescriptions

- ***Infrastructure***

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Is the existence of EHR a precondition for the ePrescription system?* | The Evaluation Of The Electronic Prescription Service In Primary Care: Interim Report on the Findings from the Evaluation in Early Implementer Sites *9th. July, 2012*[133] | In England the EHR system and Electronic Prescription Service (EPS) are fully integrated. Both the EHR and ePrescription will be part of one system. They would share data. The action of prescribing is just another event that gets added to the EHR along with other events like a test result being returned from a pathology lab or a referral being made to somewhere or a diagnosis being made as part of a consultation. They are all just different entities that would be within the database of the clinical system. The relevant information about the medications that are prescribed goes into an electronic message that is sent to the Electronic Prescription Service (EPS), and it is the EPS that makes that message available for dispensers to access.[135]<br><br>*The Evaluation Of The Electronic Prescription Service In Primary Care: Interim Report on the Findings from the Evaluation in Early Implementer Sites, 9th. July, 2012*, Page 3 states that The Electronic Prescription Service ' allows the transmission of prescription messages and digitally-signed prescriptions from primary care prescribers, via a central network and server infrastructure, the Spine, from where they can be downloaded by dispensing contractors including community pharmacists, dispensing appliance contractors and dispensing doctors.'<br><br>While most GPs generating an ePrescription will have access to an EHR, it is not an absolute precondition since there can be a paper medical record. An EHR is not a definite precondition to have an EHR for an ePrescription system. It depends on the care setting. In a GP practice it is mandatory to |

[133] The Evaluation Of The Electronic Prescription Service In Primary Care: Interim Report on the Findings from the Evaluation in Early Implementer Sites *9th. July, 2012*, available at: http://www.ucl.ac.uk/pharmacy/documents/staff_docs/EPS (last access February 2014)
[135] Interview with the EPS (HSCIC) on 6th March 2014

| Questions | Legal reference | Detailed description |
|---|---|---|
| | | have an EHR (or paper medical record) based on GMC regulations. However the same things may not be in place for community clinics or sexual health clinics or places with a limited formulary. In those care settings there is no need for a full EHR. [136] |
| | The Electronic Prescription Service Authorisation: Operating Guidance 2013/14[134] | The Electronic Prescription Service Authorisation: Operating Guidance 2013/14, makes no mention of the need for EHRs |
| *Can an ePrescription be prescribed to a patient who does not have an EHR?* | BMA's Practicing in General Practice guide, May 2013[137] | Generally there must be a medical record [although according to the BMA under certain conditions a healthcare professional can write prescriptions without access to a patient's medical records].<br><br>A patient must be registered with the NHS and have an NHS number to be issued an ePrescription. Because the patient must have an NHS number there will be an EHR for them somewhere in the NHS (in some GP). Everyone with an NHS number has to be registered with a GP somewhere. However a patient may have a paper health record. If there was no EHR relevant information that needed by law will need to be inputted (i.e. the identity of the patient –NHS number, the identity of the prescriber, and details of the medication) so that the system can generate this electronic message that becomes the ePrescription.[138] |

[134] The Electronic Prescription Service Authorisation: Operating Guidance 2013/14, http://systems.hscic.gov.uk/eps/library/authguide.pdf (last access February 2014)
[136] Interview with the EPS (HSCIC) on 6th March 2014
[137] BMA, Practicing in General Practice, May 2013, http://bma.org.uk/practical-support-at-work/gp-practices/prescribing (last access February 2014)
[138] Interview with the EPS () on 6th March 2014

- ***Access***

| Questions | Legal reference | Detailed description |
|---|---|---|
| *Do the doctors, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?* | The National Health Service (General Medical Services Contracts) Regulations 2004 as amended, (Schedule 6, paragraph 39A)<br><br>GMC - Good practice in prescribing and managing medicines and devices[139] | *The National Health Service (General Medical Services Contracts) Regulations 2004 (Schedule 6, paragraph 39A) as amended* authorises any NHS contractor (GP, hospital doctor etc.) to use the Electronic Prescription Service. A GP treating a patient will have access to his/her GP EHR or if one does not exist a paper medical record. Also in the case of an emergency or out-of-hours care a healthcare professional will have access to the patient's SCR (which can be accessed nationally).<br><br>The GMC's *Good practice in prescribing and managing medicines and devices* advises that prescribing drugs should be done 'only when you have adequate knowledge of the patient's health, and are satisfied that the drugs or treatment serve the patient's needs.' (paragraph 1a.) The guide makes clear that access to the patient's health records is necessary. However there is no specific mention of EHR. |
| *Can those health professionals write ePrescriptions without having access to EHRs?* | BMA's Practicing in General Practice guide, May 2013[140] | Under certain conditions a healthcare professional can write prescriptions without access to a patient's medical records.<br><br>In the *BMA's Prescribing in General Practice guide*, May 2013, mention is made of non-GP prescribers and their responsibility for checking interactions and taking a full drug history if they do not have access to the main clinical record.<br><br>The guidelines do not make any specific mention of ePrescriptions or EHR. However, since an ePrescription is an electronic version of a paper prescription, then there is no requirement for an ePrescription to need an EHR. |

[139] Good practice in prescribing and managing medicines and devices, http://www.gmc-uk.org/static/documents/content/Prescribing_guidance.pdf (last access February 2014)
[140] BMA, Practicing in General Practice, May 2013, http://bma.org.uk/practical-support-at-work/gp-practices/prescribing (last access February 2014)

# 3. Legal barriers and good practices for the deployment of EHRs in England and for their cross-border transfer in the EU.

- ***Good Practices for the development of EHRs in England (UK)***

  - *Health data to be included in EHRs*

    - There is an exclusion data set for the SCR (and common to the home countries), that protects various sensitive information of the patient such as data on HIV aids or sexual diseases and pregnancy terminations.[141]

    - The establishment of governance processes around any decisions about including information from other sources into an SCR. In particular setting up of a content and advisory board to examine requests for any information from other sources (other than GP records) to be included in an SCR. [142]

    - The UK law is impartial and applies equally to electronic and manual health records.[143]

  - *Requirements on the institution hosting EHRs data*

    - Institutions that host EHRs must have an appropriate licence and are subject to NHS contractual requirements.

    - From a data protection perspective institutions that host EHRs will be data controllers and as such will have to meet the requirements of the Data Protection Act. [144]

  - *Consent*

    - Use of implicit consent to create SCRs enables a greater number of SCRs to be created.[145]

    - Consent is required for each access to an SCR. Due to the nature of the sensitivity of the information it is an essential requirement that permission is asked. However, the regulations allow for access without permission in certain defined cases. The consent model for access to an SCR is very robust. This model is further strengthened in other ways: behavioural controls (ethical and professional standards required for medical professionals), contractual obligations, and disciplinary processes.[146]

    - The ICO office works very well and ensures very effective regulation and compliance with data protection requirements including consent.[147]

    - The application of the common law duty of confidence means that unless patient information is being used for their direct care, then in most cases consent is required. This requirement can be set aside but only by the Secretary of State after a heavily

[141] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.
[142] ibid.
[143] Interview with ICO on 5th March 2014.
[144] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.
[145] ibid
[146] ibid
[147] ibid

scrutinised process.[148] Note however that unlike with GP and hospital records for the SCR consent is required for each access.

- Good guidance for when implicit and explicit consent is required for sharing patient data is given by various guidelines and in particular the 2013 revised Caldicotte principles.

- *Access, authentication and authorisation*

  - There are various specific controls in place. Any organisation accessing SCRs must be authorised to connect to the NHS N3 network. There is an information governance toolkit against which organisations have to self declare and there are specific controls in there for the use of electronic information by health and social care organisations. A specific example of the Information Governance Toolkit requirement is that a privacy officer must be in place trained to interrogate the technical systems to investigate any allegations of inappropriate access to records. [149] Using an information governance toolkit, all NHS organisation must assess themselves against requirements for: management structures and responsibilities (e.g. assigning responsibility for carrying out the information governance assessment, providing staff training); confidentiality and data protection; and information security.

  - Access to an SCR via smartcard use with chip and pin works well. There is a very robust process to issuing smart cards. It can only be issued by a named registration authority - that verifies identities by documentation such as passports etc. There is a robust process for authenticating users and issuing smart cards which are unique for the user. Also there is an ability to audit its use. Each usage is electronically documented and can be traced back to the owner of the smart card. There are employment, legislation and disciplinary processes which militate against the sharing of smart cards. There is a unique identifier for each individual user who is liable for any accesses in their name.[150]

- *Liability Issues*

  - The liability for EHRs is no different than the liability with regard to the use of any other use of information in health whether paper records or electronic records. There is liability in law, liability in terms of professional conduct and liability in terms of contractual obligations. These liabilities are no different to those that existed before the creation of electronic health records. The liability for improper inputting of data into a paper record is the same as in an EHR.[151] This in some way allows EHRs to be more easily accepted and used by medical practitioners who are accustomed to using paper records. They do not have to worry about new liabilities when moving from paper based medical records to EHRs.

  - Provided that the person inputting the data has exercised due diligence and had done it in good conscience and deplored the right processes and procedures then they cannot be liable for an error which is outside of their control. But they have to demonstrate that they have taken all the right steps, that they have followed all the due process. Also their position can be defended through documentation.[152]

[148] Interview with the ICO on 5th March 2014.
[149] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.
[150] ibid.
[151] ibid.
[152] ibid.

- In hospitals regular internal and external audits are made to demonstrate compliance with NHS regulations and standards. Reminders on hospital screen savers are used to give advice on how to use medical information and the consequences of misuse. All hospital staff need to have mandatory information governance training once a year, further, new staff need to complete information governance training before they are allowed to access any system.[153]

- *Secondary use and archiving duration*

  - SCRs are held indefinitely as historical records that have been taken with regard to the clinical care of patients. When an SCR (which is in pdf format) is updated, each new record replaces the old record, but the old record is never deleted or destroyed. All records are archived (electronically) on the NHS central network (The Spine). [154] This may raise data protection concerns, however, the medical community believe that it is necessary to retain this data as a historical record especialy in case of future litigation.

  - The use of public consultations and postponement of the care.data project, involving the collection of data from GPs for secondary use indicates that these projects are being very carefully thought through.[155]

  - There are limitations on what kinds of medical information will be collected for secondary uses. Sensitive information including HIV/AIDS, sexually transmitted infections, termination of pregnancy, IVF treatment, marital status, complaints, convictions, imprisonment, and abuse by others will not be collected.

  - Although the HSCIC is empowered to collect patient data from GP surgeries and health care providers, patients have a right to object to any personal confidential data being extracted unless there is a statutory duty to share information, a court order or an overriding public interest in disclosure.

  - The Data Protection Act provides a framework to allow for the overall control of archiving. The Data Protection Act requires that personal data is not kept for longer than necessary. Any retention period must be justified. In practice this means that in some circumstances it may be that personal data can only be retained for a short period. However in other situations indefinite retention can be justified. It is all "case-by-case",[156]

- *Requirements on interoperability of EHRs*

  - The setting up of the GP Systems of Choice funding organisation ensures that although GPs can procure different IT systems there will be certain guaranteed standards.

  - By 2015 all NHS staff (or staff at any organisation who deliver care on behalf of the NHS) interacting with patients should use SNOMED CT to record and exchange coded clinical information.

[153] Interview with East and North Hertfordshire NHS Trust on 21st March 2014.
[154] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.
[155] ibid.
[156] Interview with the ICO on 5th March 2014.

- *Links between EHRs and ePrescriptions*

  - The EHR and ePrescription systems are fully integrated systems. [157]

  - Use of the unique patient identifier (in England the NHS number) – something that ties the EHR to the ePrescription (which is an electronic message sent to the Electronic Prescription Service). It is used to make sure that the ePrescription is for a particular patient, especially in cases where two or more people may have the same name.[158]

- *Other good practices*

  - Other good practices include[159] :
    - There is a good legislative framework around the use of information and the security of information.
    - There are robust technical safeguards for the security of networks, use of smart cards and authentication, use of automatic electronically generated alerts, audit trails.
    - There are good standards for the training and professional regulatory behaviour.
    - There are good contractual (employment law nature) standards.
    - There are good rules for gaining patient and public consent – making sure that the citizens of the country are informed and contributing to the debate.

- ***Potential Legal Barriers for EHRs in England (UK)***

  - *Health data to be included in EHRs*

    - The absence of more categories of data in the SCR (and other shared electronic health records), e.g. social personal care data (as in already the case in some other UK countries, e.g. the ePCS in Scotland) may limit the use of an SCR. There may be need for a clinician to know personal information such as details of family members, preferred place of death, and religious affiliation.[160]

  - *Requirements on the institution hosting EHRs data*

    - The lack of any specific legal requirement for use of a common IT system in all hospitals means that different types of EHRs may be developed in different hospitals (and therefore there may be difficulties in electronic sharing of such medical records).

    - The absence of any legal requirement for one common IT system for GPs instead of the current rules that allow different specific types of IT systems to be used. The presence of different commercial suppliers of IT systems for GP practice with each having their systems developed differently, means that the SCR developers need to talk to each supplier (to get their produce to conform to various requirements in a uniform way) when trying to extract SCR data from the GP systems onto a national spine. This involved giving suppliers money because they mainly do things that increase their profits.[161]

    - The lack of any legal obligation to use the same codes for medical data in IT systems in England, the UK home countries and in European Member States will impact on

[157] Interview with EPS (HSCIC) on 6th March 2014.
[158] ibid.
[159] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.
[160] ibid.
[161] ibid.

interoperability. Different countries with different users have developed their own different coding systems.[162]

- *Patient consent*

  - The need for consent for each access to an SCR can impede access. However this has to be balanced by the sensitivity and confidentiality of medical information.

  - There are practical difficulties in patients giving informed consent – that is, the patient should know what are the proposed uses and disclosures of personal data. [163]

  - The presence of a difficulty regarding Directive 95/46/EC in terms of the definition of consent and how consent is use in the Directive itself, i.e. the qualification of consent in the preamble and in articles such as 'unqualified', 'explicit' and 'free and informed'. There is lack of clarity as to whether in each a different meaning is intended. There should be a single definition unless different constructions are intended.[164]

- *Creation, access to and update of EHRs*

  - The need for physical smartcards to access the SCR. Such smartcards are only available to NHS England staff and hence this does not allow staff not working in NHS England (e.g. staff in other UK home countries and across borders) to access the SCR. This means that SCRs (and summary records in other UK countries) cannot be shared across borders.

  - There are practical challenges in terms of ensuring that only records that are relevant to a patient's care are shared or accessed. The move towards centralised databases of electronic health records marks a fundamental shift in the paradigm of professional responsibility for the security of patient data and about decisions to share such data. Doctors have traditionally acted as custodians of health information, sharing relevant details with others providing care and making decisions to share information with others, with or without patients' consent. The centralisation of data on shared-access databases shifts many of these responsibilities onto the person accessing the data. It is inherently more difficult for the person accessing records to know what is relevant to their role, and so restrict or avoid unnecessary invasion of the patient's privacy. Various initiatives to limit access through technological and role-based restrictions, to audit access and to allow patients to control who can access their records, to shield parts of their records from view, or to opt-out of having a shared record are advanced as means to mitigate the risks to privacy. The challenge for EU law makers is to develop legislation that reflects the new paradigm without unnecessarily stifling initiatives that promise improvements in the quality, safety and timeliness of healthcare services. [165]

- *Liability*

  - There is no specific legal liability for use of EHRs but for general liability in medical practice. This may be considered a legal barrier in terms of the law not providing certainty with regarding to the scope the extent of the liability of professionals using EHRs.

[162] ibid.
[163] Interview with the GMC, 21th February 2014.
[164] ibid.
[165] ibid.

- There may be need for legal and robust contractual provisions about the responsibilities of parties (IT systems suppliers and users) especially liability in the event of failure.[166] This relates to the issue of legal certainty for Business Continuity – how to cater for system malfunction and failure (e.g. proper testing, having regular archiving in the case of data loss) and who bears responsibility for what.[167]

- *Secondary use and archiving duration*

  - There is a lack of legal clarity with regard to archiving duration of EHRs. On one hand data protection legislation says that data should not be kept for longer than is necessary. On the other hand there is a recommendation to GPs that medical records are needed especially to provide medico-legal evidence, therefore, both the audit trail and the associated patient record should be retained indefinitely by a practice as they are the sole source of forensic evidence.

- *Requirements on interoperability of EHRs*

  - There is no specific legal requirement for interoperability of EHRs. As previously noted, there are several different commercial providers of EHR IT systems.

- *Links between EHRs and ePrescriptions*

  - While the EHR and the ePrescriptions systems are fully integrated systems, there is no legal requirement that an EHR is a precondition for the creation of an ePrescription (although in most cases an EHR will be present). Certain information is required by law for the creation of a prescription namely: the identity of the patient, the identity of the prescriber and the medication that is prescribed. This information can be keyed into a system to generate an electronic message that becomes an ePrescription.

- *Other requirements*

  - There are some challenges relating to the transfer of data about patients seeking medical care outside their home state. The challenges involved in this include the diverse implementation by nation states of Directive 95/46/EC, and the permissible variation in national law and societal norms that underpin different approaches to data protection, respect for privacy and rules for professionals. [168]

  - Privacy law and data security laws may be used as barriers by people who oppose the development of wide scale sharing for information (in national records projects such as the SCR).[169]

[166] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.
[167] Interview with East and North Hertfordshire NHS Trust on 21st March 2014.
[168] Interview with the GMC, 21th February 2014.
[169] Interview with Clinical Lead–Implemination SCR (HSCIC) on 28th February 2014.