DOI: https://doi.org./10.24163/ijart/2018/1 Available online at http://www.ijart.info/

INTERNATIONAL JOURNAL OF APPLIED RESEARCH AND TECHNOLOGY
ISSN 2519-5115

Ethical and legal issues of electronic health records in the United Kingdom

Dr. Muhammad Tahir

A project submitted in partial fulfilment of the requirements of Northumbria University for the Degree of LLM

Research undertaken in the School of Law

January 2017

ABSTRACT

Electronic health record (EHR) system is considered the fastest, effective and the most efficient method of managing patient health information and is the key element of modern healthcare provision. The EHR information and communication technology allows collection, transfer, storage and sharing of patients' health data for primary use as well as to be reused for clinical research, commissioning, public health and other secondary purposes. The health data is passed to the Health and Social Care Information Centre (an electronic health data warehouse) to allow integration of health care and research information systems, to make it available for secondary uses. The disclosure of confidential patient information without explicit consent, selling of anonymised patient health information and reports of security breach are threatening patients' trust in the system. The reuse of patients' confidential information for different purposes beyond the original purpose for its acquisition has raised ethical and legal concerns requiring an urgent effective public dialogue about the adequacy of current controls and safeguards, and opportunities related to the use of patient confidential information for purposes other than direct patient care. The thesis addresses understanding, evolution, uses, and ethical and legal aspects of EHR focusing on the issues arising from sharing of health records for secondary purposes.

DECLARATION

Originality:

I declare that the work contained in this project is my own and that it has not been submitted for assessment in another programme at this or any other institution at postgraduate or undergraduate level. I also confirm that this work fully acknowledges the opinions, ideas and contributions from the work of others.

Ethics:

The proposed research is based on secondary material or data already in the public domain (case law, journal articles, published surveys etc.). It does not involve people in data collection through empirical research (e.g. Interviews or questionnaires). The ethical risk is deemed low.

Signed: _____

Dated: _____

Table of Contents

List of Abbreviations

Abbreviation	Meaning
CCG	Clinical Commissioning Group
CDS	Clinical Decision Support
CMO	Chief Medical Officer
CPOE	Computerized Physician Order Entry
CPR	Computerized Patient Record
CQC	Care Quality Commission
CRS	Care Record Service
DICOM	Digital Imaging & Communication in Medicine
DOH	Department of Health
EHR	Electronic Health Records
EMR	Electronic Medical Records
EPR	Electronic Patient Record
HIMSS	Healthcare Information and Management Syster Society
HIPAA	Health Insurance Portability and Accountability Act
HSCIC	Health and Social Care Information System (New name for HSCIC is NHS Digital since 1 August 2016).
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
ISO	International Standards Organization
IT	Information Technology
NHS	National Health Service
NIB	National Information Board
NICE	National Institute for Health and Care Excellence
PACS	Picture Archiving Communication System
PHR	Personal Health Record
SCR	Summary Care Record
UK	United Kingdom
US	United States of America

List of Figures

Acknowledgments

I would like to express my sincere appreciation and gratitude to my dissertation supervisor, Kristina Swift, who made this work possible, and has advised and supported me during completion of my work.

Chapter 1: Introduction

In this chapter, an overview of EHR and issues related to secondary use of patient health information are highlighted. The reason and scope of the thesis is described.

NHS England has a set target to implement EHR and make health records largely paperless by 2020.[1] The Government intends to include patients' information in EHR about clinical history, life style and care preferences; updated in real time and accessible to health and social care providers as well as to patients.[2]

In the last few years, some local and national schemes were implemented to extract personal confidential data (PCD) from care provider (GP surgeries and hospitals) computer systems and send to Local Care Records, Summary Care Record (SCR) and Health and Social Care Information Centre (HSCIC). Some of these data extractions are for direct patient care (primary purpose), for example to help the patient if a patient gets admitted to an accident and emergency department of a hospital elsewhere in the country. Some are not for direct patient care but for other purposes such as research and commissioning, that is not the purpose the data was originally acquired for (secondary use). Do we have legal and ethical justifications for such uses? Should a patient be able to opt out? This also exacerbates patients' concerns when patients are not aware of what happens with their data, or what data is safe and what is not.[3] The sharing or linking of patients' health information without patients' knowledge or consent jeopardizes autonomy of the patient and builds distrust in the system. The lack of privacy and confidence in healthcare system might lead to patients' withholding vital information from their clinicians and compromise treatment, which is neither beneficial for the patients nor to the interest of the public.

[1] NHS England, *Five Year Forward View* (2014).
[2] Department of Health *Personalised Health and Care 2020* (2014).
[3] Deven McGraw, 'Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data' (2013) 20(1) JAMIA 29.

The healthcare organisations are registered with the Information Commission Office as Data Controllers and are held accountable in case of loss of personal or confidential data. The data can be de-identified or anonymised (after stripping of all identifiable elements) or Pseudo-anonymised (authorised persons can identify individual records). There is no common law requirement to obtain consent for the use of anonymised data. The DPA 1998 is not applicable as there can be no significant threat to the patient's privacy from anonymised data. However, DPA 1998 requirement must be fulfilled to process the data and the patient might have rights under other headings of the law such as breach of confidence or the law of contract, for example *R v Department of Health ex parte Source Informatics Ltd*.[4] The case will be discussed in detail in chapter 7 to avoid repetition, but it is an example of such a situation. There is increasing public awareness of violation of privacy regarding health data and easiness of combining and using data for re-identification, which was meant to be kept safe that may not remove patients' concerns by de-identification of their health data.[5] There were reports of selling of de-identified (anonymised) data to the pharmaceutical and other companies that have also raised ethical questions about selling of health data, and concerns of public and healthcare professionals regarding ownership of the data. The other media reports such as 'Hospital records of all NHS patients sold to insurers'[6] and 'NHS England Patient Data uploaded to Google server'[7] have caused widespread disquiet among the public.

Informed consent provides legal basis for sharing any medical records (DPA 1998). Healthcare professionals use implied and explicit consent to access patients' health records. For disclosure of information, 'explicit consent' is

[4] [1999] 4 AllER 185.
[5] Kathleen Benitez and Bradley Malin, 'Evaluating Re-Identification Risks with Respect to the HIPAA Privacy Rule' (2010) 17(2) JAMIA 169.
[6] Laura Donnelly, 'Hospital Records of all NHS Patients Sold to Insurers' The Telehraph 23 February 2014 <http://www.telegraph.co.uk/news/health/news/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html > Accessed on 17 January 2017.
[7] Randeep Ramesh, 'NHS England Patient Data 'uploaded to Google server', Tory MP says' The Guardian 3 March 2014 <https://www.theguardian.com/society/2014/mar/03/nhs-england-patient-data-google-servers > accessed on 07 January 2017.

safer than implied consent. However, this right can be overridden in the presence of clear legal reasons. Where sharing of patient information is part of the care process and the patient is made aware of the opt out option or option to refuse disclosure, implied consent is the policy, endorsed by the relevant bodies. The NHS plan to balance the patient confidentiality issues and improvement in the quality of service is a difficult balancing task. For clinical staff, in situations where patients lack capacity, in cases of children and where clear guidance is not available, guidance should be obtained before disclosure. Guidance regarding disclosure can be sought from various medical organizations including General Medical Council (GMC), British Medical Association (BMA), medical defence organizations and Clinical Commissioning Groups (CCGs).

A comprehensive EHR system is designed to store large amounts of highly detailed legible retrospective, prospective and concurrent clinical information (clinical history, physical examination, radiology, laboratory and other clinical investigations and medical management) securely and accurately, in systematized compact fashion, to be easily and rapidly accessible by the authorized multiple healthcare professionals simultaneously at different locations and electronically transferable among healthcare providers, to support continuity of efficient and high quality integrated healthcare. The traditional paper medical records differ from EHR as they do not present these characteristics. The paper medical records are usually centrally located, illegible or poorly legible hand written ‘forms and charts’ in a department or institution building. EHR can reduce problems of wrong prescription and doses of medicines as well as adverse drug reactions. Despite all these advantages of EHR over paper medical records; the ethical and legal problems associated with patient information use such as privacy, confidentiality and security breaches are real challenges for implementation of

EHR.[8,9,10] Although easy and rapid accessibility makes EHR inherently more vulnerable to security breaches as compared to paper medical records but ethical and legal issues related to disclosure and sharing of health information apply to both EHR as well as paper records.

The new emerging legal issues related to EHR include clinicians' responsibility to review all EHR accessible clinical summaries from various physicians and institutions; consequences of disregarding EHR generated alerts and overriding clinical support decisions. Sitting has proposed 10 basic "rights" for all physician EHR users, some of these include right to uninterrupted EHR access, right to see all data required to provide safe and effective care, right to a succinct patient summary and right to override computer-generated alerts.[11]

The UK's main pieces of relevant legislation which cover creation, storage and sharing or disclosure of health information include Common Law Duty of Confidentiality and Duty of Care, Human Rights Act 1998 (HRA 1998), DPA 1998, Section 251 & section 252 of the National Health Service Act 2006, Health and Social Care Act 2012, Access to Health Records Act 1990, Access to Medical Records Act 1988, the Computer Misuse Act 1990 and other health Acts (Sexual Health Records Act), Freedom of Information Act 2000, Electronic Communication Act 2000, Mental Capacity Act 2005, The Access to Medical Reports Act 1988, The Terrorism Act 2000 (Section 19), Environmental Information Regulations 2004, Re-use of Public Sector

[8] Penny Duquenoy, Carlisle George and Kai Kimmpa, *Ethical, Legal and Social Issues in Medical Informatics* (IGI Global 2008).
[9] Carlisle George, Diane Whitehouse and Penny Duquenoy, '*eHealth: Legal, Ethical and Governance Challenges'* (Springer 2012).
[10] Laurinda Harman, Cathy Flite and Kesa Band, 'Electronic Health Records: Privacy, Confidentiality and Security' (2012) 14(9) VM 712.
[11] Dean Sittig, Hardeep Singh, 'Rights and Responsibilities of Physician Users of Electronic Health Records' (2012) CMAJ <https://sbmi.uth.edu/nccd/research/sharpc/pdfs/Physicians_Professional_rights-CMAJ_v9-formatted.pdf> accessed on 5 December 2016.

Information Regulations 2005, Health and Social Care Act 2008, and NHS (Venereal Diseases) 1974 Regulations. The most relevant laws that govern secondary uses of personal data include DPA 1998, Common law of confidentiality, HRA 1998, Section 251 and Section 252 of National Health Service Act 2006 (section 60 and section 61 of the Health and Social Care Act 2001 were replaced by these sections), and Health and Social Care Act 2012.

In conclusion, three categories of issues related to sharing of health records for secondary purposes have been identified. Issues of first category are consent, its alternatives and confidence. The second category is opting out, its grounds, provision and ramifications. The third category is public interests, altruism and social solidarity. The thesis will address understanding, evolution, uses, ethical and legal aspects of EHR; and will focus on sharing of health records for secondary purposes and ethical and legal issues arising from its secondary use. The chapters that follow will address the sets of issues including health data and its secondary uses; balancing competing interests - individual versus society interests, public interest in maintaining confidence versus public interest in disclosure; sources of confidentiality and protections. The United Kingdom consist of England, Scotland, Wales and Northern Ireland – four home countries; having separate national health systems and national information governance structure. To narrow the scope of this thesis, the major emphasis will be on EHR systems in England.

Chapter 2: EHR, definitions, acronyms, data processing and DPA 1998

This chapter presents definition of EHR and interchangeably used acronyms with EHR. EMR (Electronic Medical Record), EPR (Electronic Patient Record), PHR (Personal Health Record) and CPR (Computerised Patient Record) are variously terminologies used regarding patients' health records and are sometimes confusing. Definitions of record, information, data, data subject, data controller, personal data, sensitive personal data, health record, data processing and requirements for data processing under DPA 1998 are provided as a basis to understand DPA 1998 and its application to confidentiality.

2.1. Record

A record is 'information, created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.'[12]

2.2. Information, data

Information is defined as the:

> output of some process that summarises, interprets or otherwise represents data to convey meaning, whereas, data is defined as the 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.[13]

Information can be identifiable (when used alone or combined with other available information, may reasonably be expected to identify an individual) or non-identifiable (when used alone or combined with other available information, does not identify an individual).[14]

[12] ISO standard, ISO 15489-1:2016. Information and documentation – Records management. <http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542> accessed on 10 January 2017.

[13] The Minister for the Cabinet Office, '*Open Data White Paper*' (CM 8353, June 2012. <https://data.gov.uk/sites/default/files/Open_data_White_Paper.pdf> accessed on 11 January 2017.

[14] Government of Canada Panel on Research Ethics, 'Privacy and Confidentiality'. <http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter5-chapitre5/ > accessed on 7 January 2017.

The information can also be further categorised in to **anonymous** (never had identifiers linked with it), **anonymised** (direct identifiers are stripped of and the code to re-identify is not kept to allow future re-linkage), **coded** (direct identifiers are removed with a code and re-identification of the particulars is possible by accessing the code), **directly identifiable** (a specific individual can be identified through direct identifiers) and **indirectly identifiable** (a combination of indirect identifiers such as date of birth, place of birth, place of residence can reasonably be expected to identify an individual).[15] Anonymous information is relatively safe and has very low risk for security but it is less valuable for research purposes.[16]

2.3. Data Subject

Under section 1(1) of the DPA 1998, the 'data subject' is defined as, 'an individual who is the subject of personal data'. In the medical context patient is a 'data subject'.

2.4. Data Controller

Under section 1(1) of the DPA 1998, the 'data subject' is defined as:'…a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.'

In the medical context, GP practices, NHS Trusts and so on will be data controllers; and under section 4(4) will have 'the duty of a data controller to comply with the data protection in relation to all personal data with respect to which he is the data controller'

[15] ibid
[16] ibid

2.5 Personal data

Personal data is defined under section 1(1) of the DPA 1998 as:

> …data which relate to a living individual who can be identified –
> (a) from those data, or
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2.6. Sensitive personal data

Under section 2 of the DPA 1998, the definition of sensitive personal data is wide. Section 2(e) is the relevant part, serving the purpose of definition in health record context. Sensitive personal data is personal data related to '…physical or mental health or condition'.

For practical purposes, the personal data in the health record is sensitive personal data. The key point is 'sensitivity of personal data'. For example, patients might wish to keep their data private, such as prescribed tranquillizers or oral contraceptive pills, information about alcohol or substance abuse, sexual or mental health, termination of pregnancy because deliberate or accidental disclosure of such personal information can cause distress or embarrassment with potential serious consequences. Employers, banks or insurance companies might get access to the sensitive personal data and patients might lose their trust in the system. The fears of potential disclosure of sensitive personal data and perception of loss of control on personal data are growing after recently published reports that have raised issues of consents and its alternatives, anonymisation, confidence and opt-out. These issues are discussed in more detail in the following chapters.

2.7. Patient record

Per Bemmel & Musen, 'The patient record is an account of a patient's health and disease after he or she has sought medical help. The record should usually contain findings, considerations, test results and treatment information related to the disease process.'[17]

2.8. Health record

The DPA 1998 defines health record in section 68(2) as

> any record which –
> (a) consists of information relating to the physical or mental health or condition of an individual, and
> (b) has been made by or on behalf of a health professional in connection with the care of that individual.

This will include EHR as well as manual records.

The meaning of health professional is given in section 69 of DPA 1998 that includes registered medical practitioner, registered dentist, registered dispensing optician, registered pharmacist, registered nurse or midwife and so on.

2.9. Medical record

A medical record whether in paper or electronic format is a chronological written account of a patient's medical history containing information of patient's complaints, physical examination findings, medical diagnostic test results, medications and therapeutic procedures.[18]

For practical purposes, a medical record is health information collected by a health professional for patient care or in more simple words, a record related to patient care. The terms health record and medical records are used interchangeably.

[17] Jan Bemmel and Mark Musen, '*Handbook of Medical Informatics*' (Springer 1997).
[18] <http://www.dictionary.com/browse/medical-record> (accessed on 2 Dec. 16)

2.10 Structure and content of patient record

The standards for the structure and content of patient records are outlined in NHS document 'Standards for the clinical structure and content of patient records' that apply to paper records as well as to EHR.[19]

The Department of Health Code of Practice 'Records Management Code of Practice for Health and Social Care 2016' confirms, at paragraph 1, that the guidelines in the Code of Practice apply to NHS records regardless of the media holding them and at paragraph 9, that for the purposes of the Schedule 1 of the Public Records Act 1958, the records of NHS organisations are public records. The Code, at paragraph 5 gives examples of functional areas and the format of the records.

2.11. Electronic Health Record (EHR)

There is no universally accepted definition of EHR. The EHR is longitudinal (includes long term record of health care, possibly from birth to death), comprehensive (includes care records of all types of episodes from multiple types of care providers, not just one specialty or one event), patient centered (related to one subject of care at one or multiple care providing institutions, not only to an event or episode at one institution) and prospective (includes record of not only previous events but also prospective information that is plans, orders, evaluations and goals).[20]

[19] HSCIC, Academy of Medical Royal Colleges, 'Standards for the clinical structure and content of patient records' (2013) HSCIC. <https://www.rcplondon.ac.uk/projects/outputs/standards-clinical-structure-and-content-patient-records> accessed on 10 January 2017.

[20] Sebastian Garde, Petra Knaup, Evelyn Hovenga, and others, 'Towards Semantic Interoperability for Electronic Health Records' (2007) 46(3) Methods of Information in Medicine 332.

Healthcare Information Management System Society (HIMSS) defined EHR as:

> a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunization, laboratory data and radiology reports. The EHR automates and streamlines the clinician's workflow. The EHR has the ability to generate a complete record of a clinical patient encounter – as well as supporting other care-related activities directly or indirectly via interface – including evidence-based decision support, quality management, and outcomes reporting.[21]

The International Standards Organization (ISO) defined EHR as:

> … a repository of information regarding the health of a subject of care in computer processable form, stored and transmitted securely, and accessible by multiple authorized users. It has a commonly agreed logical information model which is independent of EHR systems. Its primary purpose is the support of continuing, efficient and quality integrated healthcare and it contains information which is retrospective, concurrent and prospective.[22]

In simple words, EHR is systematized electronically stored patient and population health information in digital format.[23]

2.12 Electronic Medical Record (EMR)

Electronic Medical Record (EMR) is an electronic record of an individual's health information, generated, stored and managed by authorised clinicians/ healthcare professionals within one healthcare organization. Sharing of the patients' data electronically among different providers and Decision Support are the important features of EHR differentiating it from EMR.

[21] HIMSS, 'Electronic Health Records.' <http://www.himss.org/library/ehr> accessed November 10, 2016.
[22] ISO TR 20514:2004 Health Informatics – 'EHR Definition, Scope, & Context.' <http://tc215.behdasht.gov.ir/uploads/244_514_ISO_TR_20514_2005(E)> accessed on 24 November 2016.
[23] Tracy Gunter, Nicolas Terry, 'The Emergence Of National Electronic Health Record Architectures In The United States And Australia Models, Costs and Questions' (2005) 7 (1) Journal of Medical Internet Research e3.

2.13. Computerised Patient Record (CPR)

Computerised Patient Record (CPR) is more accurate term than EHR serving the same purpose but EHR is globally accepted and more popular term than CPR.

2.14. Electronic Patient Record (EPR)

Electronic Patient Record included patient's only relevant medical information instead of lifelong records and is not a globally popular term.

2.15. Personal Health Record (PHR)

Personal Health Record is patient's personal record managed and controlled by the patient, guardian or carer. PHR can be connected to the patient's EHR (Tethered PHR).

EHR embraces wide characteristics whereas EMR and EPR are components of EHR. Although EHR seems to be globally accepted generic term for patients' electronic care systems; CPR, EMR and EPR are still being used in some parts of the world.

2.16. Processing of Data

Under section 1(1) of the DPA 1998 'processing' of 'information or data', is defined that 'means':

> obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the information or data, including –
> (a) organisation, adaptation, or alteration of the information or data,
> (b) retrieval, consultation or use of the information or data,
> (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
> (d) alignment, combination, blocking, erasure or destruction of the information or data.

For the medical purposes and for the purposes of the thesis, this definition would cover disclosure of confidential information.

2.17. Data Protection Act 1998

The DPA 1998 was passed to implement European Directive 95/46/EC and became effective in March 2000. The Information Commissioner's Office (ICO) is responsible for overseeing and enforcement of the Act. This is related to the processing of all personal data of a living individual that means collecting, storing, sharing, using, disclosing or doing anything with any information of a living individual, and within medical context it will cover all aspects of health records. Any processing must meet one of the requirements of schedule 2; and for sensitive personal data, one of the conditions of schedule 3 of the Act must be satisfied in addition to the obligation that any processing must be as per the 8 data protection principles set out in Schedule 1, Part 1 of the DPA 1998.

The Eight Data Protection Principles

The main points of principles include that 'personal data' should be

- processed fairly and lawfully and shall not be processed until one of conditions from Schedule 1; and in case of sensitive personal data, one of the conditions from Schedule 2 are met.
- obtained and processed for limited lawful purposes and further processing should not be incompatible with those purposes.
- 'adequate, relevant and not excess'
- accurate and where necessary kept up to date.
- kept not longer than necessary.
- processed per data subject's rights under the Act.
- secured after taking appropriate security measures
- not transported to countries outside European Economic Area without adequate protection.

For the purposes of health data processing the most commonly relied upon conditions include:

Schedule 2 conditions:

- that the consent has been obtained from the data subject
- that processing is necessary for legal obligations.

Schedule 3 conditions:

- the processing is necessary for 'the vital interests of the data subject or another person'.
- the processing is undertaken by a health professional and is necessary for 'medical purposes', that 'includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services'.

2.18. Summary

Definitions related to health records, content and processing are discussed. Key point is that both EHR and paper based records are subject to the common duty of confidentiality. Health records must be accurate, should include relevant clinical findings, diagnostic and therapeutic management, information provided to patients and structured as per the national standards as discussed in components and standards chapters. Processing of the health data should be as per DPA 1998 requirements. Patients must be aware of storage and sharing of their health data and should have access and controls on the limits of their shared data as well as have the opportunity to opt out. There are legal obligations for retention of records and Department of Health NHS Code of Practice 'Records management' (2006)[24] should be followed.

[24] Department of Health, 'Records management: NHS Code of Practice' (2006) DH London.

Chapter 3: Historical development of EHR

Historical development of EHR, its implementation in UK and an overview of EHR related issue are discussed in this chapter. Brief history of NHS is given in the beginning of the chapter.

3.1. Brief history and structure of National Health Service (NHS)

On launching a review of NHS IT, Professor Wachter said:

> The NHS is one of the world's largest health and healthcare systems, and one of its largest employers. It's essential that information technology across the NHS works well and can perform the tasks needed to deliver high quality, safe and efficient care….[25]

NHS started on 5th of July 1948, funded by the tax system, with principles of free healthcare for everyone at the point of use and access based on clinical needs, not on ability to pay.[26]

Multiple attempts were made to improve the quality of service by changing the structure of NHS. The Health and Social Care Act 2012 brought major reforms to the structure of the health services in England; the replacement of primary care trusts (PCTs) by the GP led 211 Clinical Commissioning Groups (CCGs) from April 2013 onwards was one of these recent changes to the structure of the NHS.[27] The following 3 different versions of diagrams show NHS structure before and after April 2013.

[25] DH Media Centre, 'Leading expert launches review of NHS IT' 8 February 2016. <https://healthmedia.blog.gov.uk/2016/02/08/bob-wachter/ > accessed on 10 January 2017.
[26] Geoffrey Rivett, 'National Health Service History' < http://www.nhshistory.net > accessed on 10 January 2017.
[27] ibid

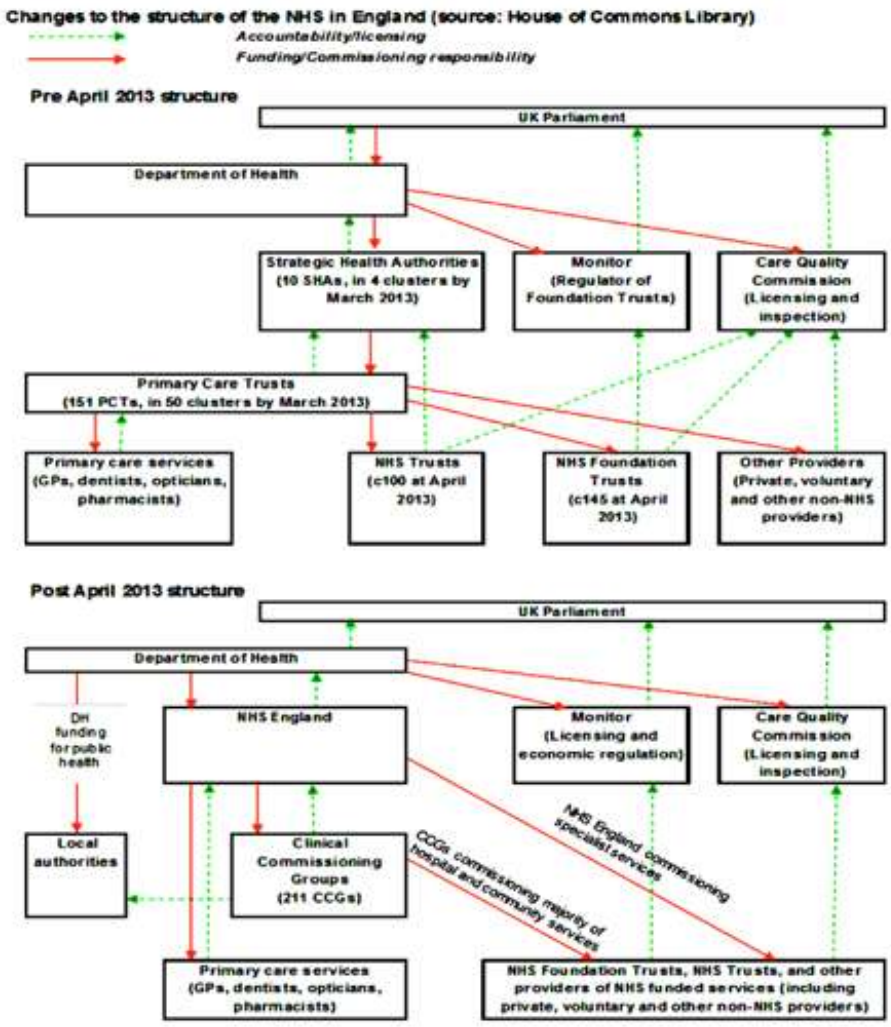


Figure 3.1- Changes to the structure of NHS in England (Source: HOC Library)[28]

[28] Thomas Powel, 'The structure of the NHS in England' (House of Commons Library Briefing Paper CBP 07206, 2016) <http://www.nhshistory.net/Parliament%20NHS%20Structure.pdf >

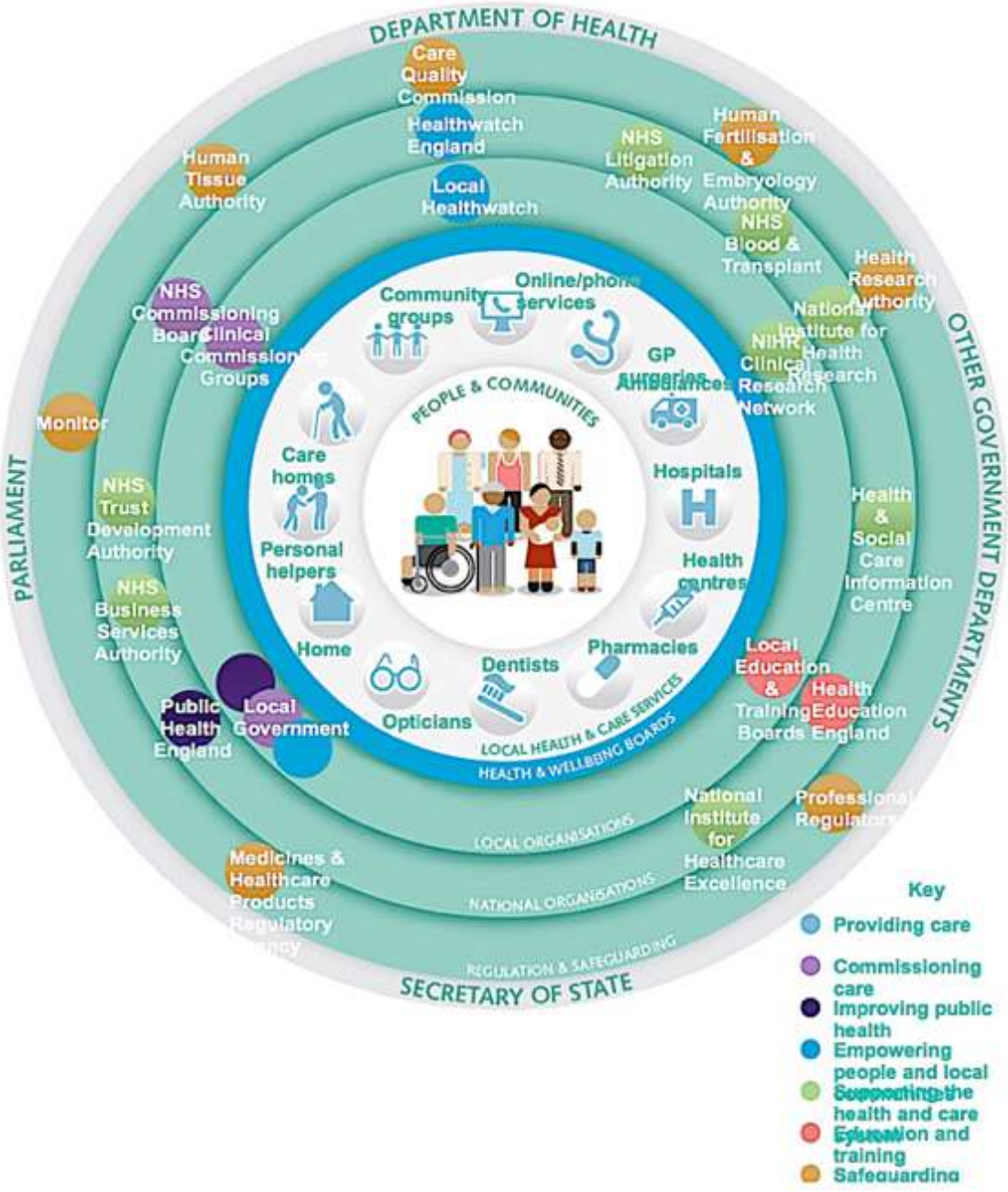


Figure 3.2 – The healthcare system in England from April 2013 (Source DH)[29]

[29] Department of Health, 'Guide to the Healthcare System in England' (2013). <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/194002/9421-2900878-TSO-NHS_Guide_to_Healthcare_WEB.PDF>

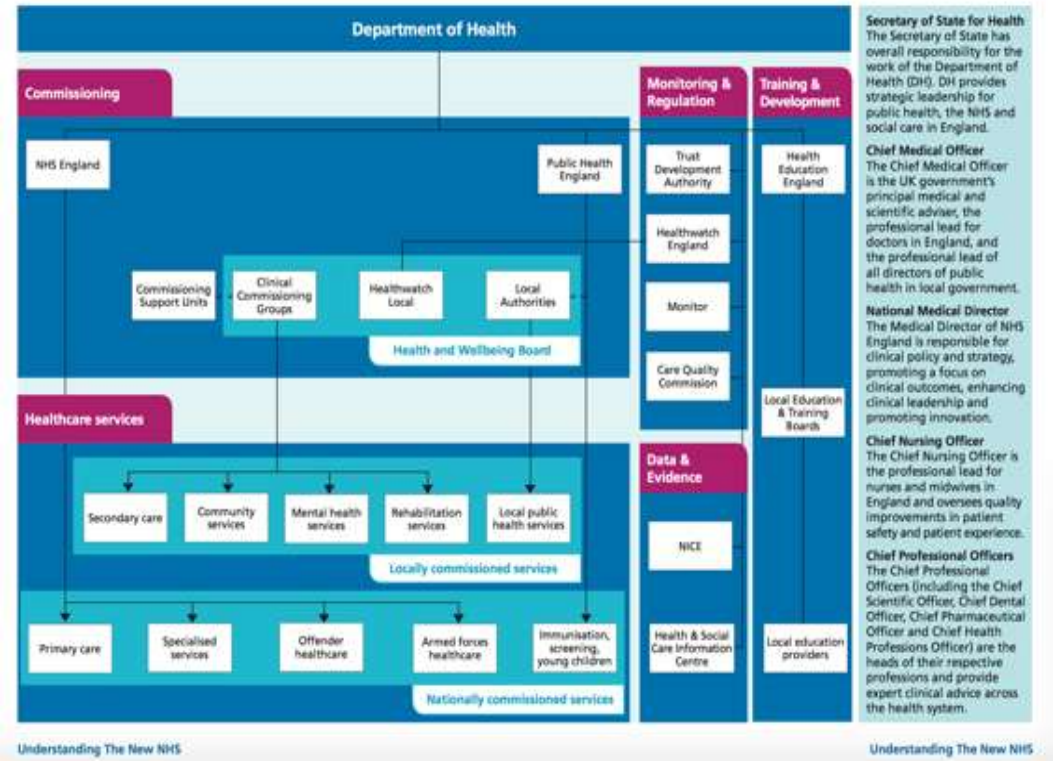


Figure 3.3: Structure of the NHS in England (Source - NHS England)[30]

CCGs plan and pay for local health services and can commission NHS hospitals, private sector providers, charities, social enterprises or other services meeting NHS standards.[31] The Care Quality Commission (CQC) being independent regulator for health and social care in England, inspects and monitors health care services including hospitals, GP surgeries, care homes and dentists to ensure provision and continuous improvement of compassionate, safe, effective and high quality care.[32]

[30] NHS England, 'Understanding the New NHS' (2014). <https://www.england.nhs.uk/wp-content/uploads/2014/06/simple-nhs-guide.pdf>
[31] NHS England, 'About NHS England' (2016) <https://www.nhs.uk/about/> accessed on 6 January 2017.
[32] The Care Quality Commission, 'Who we are' <http://www.cqc.org.uk/content/who-we-are> accessed on 6 January 2017.

The National Institute for Clinical Excellence (NICE) was established in 1999 as a special health authority to improve the quality and availability of NHS treatment and care.[33] It merged with Health Development Agency in 2005 and its name was changed to the National Institute for Health and Clinical Excellence and started developing public health guidance.[34] From April 2013, its name changed again to National Institute for Health and Care Excellence and became a Non-Departmental Public Body (NDPB) with new role for developing quality standards and guidance in social care because of reorganization of NHS in England, outlined in the Health and Social Care Act 2012.[35]

The Healthwatch England is a statutory body introduced by the Health and Social Care Act 2012, to promote patients' interests nationally by understanding their needs, experiences and concerns and speaking out on their behalf as well as the possibility of providing an advocacy service for people making a complaint using the NHS complaint process.[36] The CQC can take actions on the recommendation of Healthwatch England.

NHS Choices is an official primary website of NHS England for public information about health conditions and was set up in 2007. It provides location of health services, e-Referral Service to book an appointment at a hospital or a clinic of patients' choice and other information.[37]

NHS Improvement is operational organisation since 1 April 2016, for Monitor, NHS Trust Development Authority, Patient Safety, Advancing Change Team and Intensive Support Teams; responsible for overseeing NHS foundation trusts (not-for-profit public benefit corporations) and NHS trusts as well as

[33] NICE, 'About' < https://www.nice.org.uk/about> accessed on 6 January 2017.
[34] Ibid.
[35] ibid
[36] Healthwatch England, 'About us' < http://www.healthwatch.co.uk/about-us> accessed on 6 January 2017.
[37] NHS choices, 'About' <http://www.nhs.uk/aboutNHSChoices/Pages/NHSChoicesintroduction.aspx> accessed on 6 January 2017.

independent NHS funded care providers.[38] Before April 2016, Monitor was an executive non-departmental public body of the Department of Health, established since 2004 under the Health and Social Care (Community Health and Standards) Act 2003. Monitor's responsibilities included authorising, monitoring and regulating NHS foundation trusts to ensure sustainable quality care provision, protection of patient choice and prevention of anti-competitive behaviour that is against the patients' interests, as well as continuation of essential health care services by supporting commissioners if a provider gets in to serious financial difficulties.

Social care services such as home care, residential care, support for carers and financial support are organized by 152 local authorities. Public Health England became operational on 1 April 2013 as an executive agency of the Department of Health after reorganisation of the NHS in England drawn in the Health and Social Care Act 2012 and replaced the Health Protection Agency, the National Treatment Agency for Substance Misuse and some other health bodies.[39]

There are several independent regulators for health care professionals including the General Medical Council (GMC) for doctors; the Nursing and Midwifery Council (NMC) for nurses and midwives, the General Dental Council (GDC) for dental professionals; the General Pharmaceutical Council (GPhC) for pharmacists and technicians; the General Optical Council for optometrists, dispensing opticians and student opticians; and the Health and Care Professions Council (HCPC) for wide range of professions such as occupational therapists, art therapists, speech and language therapists, dietitians, hearing aid dispensers, biomedical scientists, clinical scientists, podiatrists and chiropodists.[40]

[38] Department of Health, 'NHS Improvement. About us'<https://improvement.nhs.uk/about-us/who-we-are/> accessed on 6 January 2017.
[39] Department of Health, 'Structure of Public Health England (2012). <http://www.rcpsych.ac.uk/pdf/Structure%20of%20Public%20Health%20England.pdf> accessed on 6 January 2017.
[40] NHS England, 'Understanding the New NHS' (2014) < https://www.england.nhs.uk/wp-content/uploads/2014/06/simple-nhs-guide.pdf> (accessed on 6 January 2017).

3.2. History and structure of Medical Records in England

In fifth century B.C. Hippocrates developed the first known medical record with two goals that are still valid:

- 'A medical record should accurately reflect the course of disease.
- A medical record should indicate the probable cause of disease.'[41]

The history of EHR goes back to 1960's when Professor Larry Weed introduced problem oriented medical record (POMR) design in to medical practice.[42] The POMR model had 3 major components that included database, problem list and progress notes. The database consisted of past medical history such as allergies, vaccinations, screening and operations; social history; family history, and administration (registration and demographics). The second component of POMR was problem list that included both active and inactive problems. The third component, progress notes contained subjective (history and symptoms), objective (clinical findings and test results), assessment (diagnosis) and plan (treatment including medication and therapy; follow-up and referral). Following schematic diagram is adapted from Benson (2009)[43] and recreated illustrating the concept of POMR design.

[41] Jan Bemmel and Mark Musen, '*Handbook of Medical Informatics*' (Springer 1997)
[42] Lawrence Weed, 'Medical Records That Guide and Teach' (1968)278(11) NEJM 593.
[43] Tim Benson, 'Principles of Health Interoperability HL7 and SNOMED' (Springer 2009).

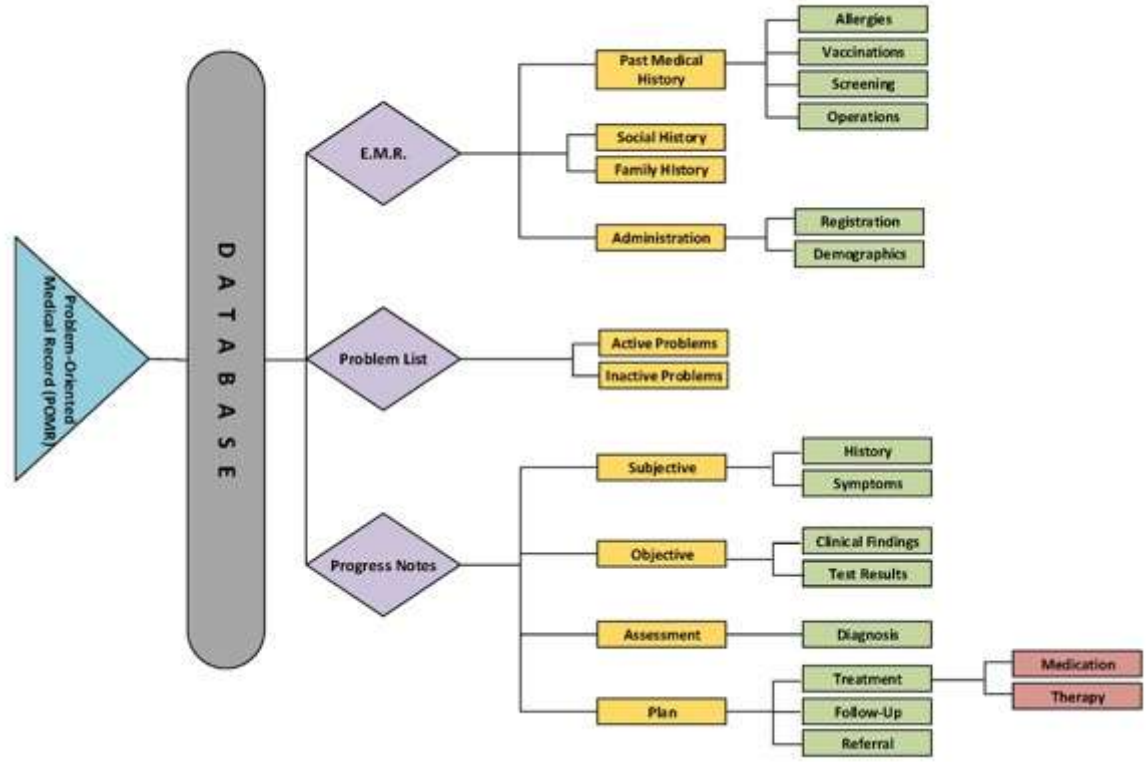


Figure 3.4: Conceptual Structure of POMR. (Source Benson 2009).

In England, several NHS Trusts and hospitals introduced information systems at individual levels in 1970s and 1980s. Wessex Regional Health Authority (WHRA) started Regional Information Systems Plan (RISP) in 1984 and abandoned in 1990. Seven NHS Trusts ran Hospital Information Support System (HISS) from 1988 to 1995 which were examples of unsuccessful IT healthcare system.[44]

3.2.1. NHS Information Management and Technology (IM&T)

IM & T was the IT strategy of NHS presented in 1992 recognising five main principles for the use of information in the healthcare and introducing key

[44] Oliver Campion-Awward, Alexander Hayton, Leila Smith and others, 'The National Programme for IT in the NHS: A Case History' (UOC 2014) <https://www.cl.cam.ac.uk/~rja14/Papers/npfit-mpp-2014-case-history.pdf> accessed on 3 Dec 2016.

pieces of infrastructure such as NHS Number, shared NHS administrative registers (NHSARs) and the NHS-wide information network NHSnet.[45] The five principles were that information should be person based; IT systems should be integrated; information should be derived from existing operational systems; information should be secure and confidential; and information should be shared across the NHS.[46]

In 1998 Labour Government introduced '1998 IM&T strategy' (a combination of strategic vision and implementation plan), identifying several strategic aims and setting forth several implementation targets. The targets included the aim of: computerising and connecting all GP surgeries to NHSnet by 2002, electronically communicating all radiology reports by 2003, computerising all NHS prescription and booking systems by 2004, ensuring installation of level-3 EPR systems and introducing nationwide telemedicine services by 2005.

The Department of Health published guidance on "**The Protection and Use of Patient Information**" in March 1996.[47] This guidance demanded that only minimum necessary patient information should be used when its use was justified and wherever possible, it should be anonymised. **Confidentiality concerns** were raised from early 1990 onwards [48,49,50] but the government did not address this issue in '1998 IT&M strategy' and the confidentiality debate was limited to the 1997 Caldicott review.[51]

The **Caldicott review** was commissioned by the CMO of England, setting out several principles aimed at protecting 'patient-identifiable information'. The

[45] ibid
[46] ibid
[47] Department of Health,' Protection and Use of Patient Information: Guidance on confidentiality'. (March 1996).
[48] Alison Tonks, 'Information Management and Patient Privacy In The NHS' (1993)307 BMJ 1227
[49] Ross Anderson, 'NHS-Wide Networking and Patient Confidentiality' (1995) 5 BMJ 31.
[50] Simon Smith and Ian Denley, 'Privacy in Clinical Information Systems in Secondary Care' [1999] BMJ 1328
[51] Campion-Awward (n 44).

Caldicott review[52] identified following 6 General Principles and made 16 detailed recommendations.

1. Justify the purposes of the proposed use of patient-identifiable information.
2. Don't use patient–identifiable information unless it is necessary.
3. Use the minimum necessary amount of patient-identifiable information.
4. The patient-identifiable information should be accessed on a strict need-to-know basis.
5. Make sure that everyone with access to patient-identifiable information is aware of their responsibilities and obligations.
6. Ensure that every use of patient identifiable information is lawful and someone in each organization is responsible for compliance of law with regards to handling of patient identifiable information. (The people with these responsibilities in each organisation are known as 'Caldicott Guardians').

3.2.2. National Programme for IT (NPfIT)

In 2002, the Government initiated, the UK's largest public sector IT programme "National Programme for IT" (NPfIT) in NHS which was dismantled in 2011 due to delays, escalating costs (total spent was estimated at closer to £10 billion, whereas originally it was budgeted at £6 billion), opposition of stakeholders and various implementation issues including criticism on top-down implementation policy.[53]

Despite its failure, the NPfIT had some successes including online appointment booking (Choose and Book), secure emails, digital imaging and GP to GP record transfer and so on. NHS Connecting for Health (CfH) was created in 2005 replacing the former NHS Information Authority to deliver NPfIT programme. Five local service providers (LSPs) covering different regions of England supported NPfIT with implementation of various national initiatives. National Application Service Providers (NASPs) were appointed to manage services common to all users (Choose and Book – Atos Origin and

[52] Department of Health, The Caldicott Committee, Report on the Review of Patient-Identifiable Information (December 1997). <http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf> accessed on 15 November 2016.

[53] Campion-Awward (n 44).

Cerner; NHS Care Records Service and N3 – BT; NHSmail – Cable and Wireless).

The national initiatives of NPfIT included NHS Care Records Service, Spine, NHS Electronic Prescription Service, Choose and Book, Picture Archiving and Communication System (PACS), NHSmail, GP2GP transfer, New National Network, GP System of Choice (GPSoC), Quality Management and Analysis System (QMAS) and the Quality and Outcomes Framework (QOF) and HealthSpace. The HealthSpace was a patient portal to record medical data including blood pressure, blood sugar levels and so on, to view their Summary Care Record (SCR) and to make hospital appointments but the service was shut down in December 2012 due to lack of interest and all HealthSpace Data was destroyed in April 2013, in compliance with the DPA 1998.

3.2.3. Health and Social Care Information Centre (HSCIC)

HSCIC replaced NHS Connecting for Health (CfH) by the UK coalition government on 31st March 2013. The Health and Social Care Information Centre (HSCIC) name changed to NHS Digital from 1 August 2016.[54]

The HSCIC, under the powers of the Health and Social Care Act 2012, can extract and share personal confidential data (PCD) from patients' health records without patient consent.

Jamie Grace and Mark Taylor argued that there is a legal duty, in so far as it is practicable, to consult individuals before their confidential information is used for secondary purposes, as the Health and Social Care Act 2012 will not easily displace this legal duty.[55] If any legitimate aim cannot be met effectively without intrusion, the courts will require that interference with a fundamental

[54] NHS Digital, 'NHS Digital Name Change' (2016) <http://content.digital.nhs.uk/sus/whatsnew> accessed on 6 January 2017

[55] Jamie Grace and Mark Taylor, 'Disclosure of Confidential Patient Information and the Duty to Consult: The Role of the Health and Social Care Information Centre'. (2013) 21 Medical Law Review 415.

right or freedom must be lawful, necessary, and **proportionate** in pursuing a legitimate objective.[56]

In a study 'on the relationship between preference and acceptability in the use of personal data for health research', it was found that 'there is reason to believe that the public are willing to accept access to confidential health information for secondary purposes without explicit consent as appropriate, if certain conditions are met, even if this would not be their preference'.[57]

3.2.4. Summary Care Record (SCR)

The SCR was the key component of NPfIT. The purpose of SCR was to make a centralised comprehensive electronic record of patients' essential health information including medications, allergies and adverse reactions to drugs; to be readily available to authorised primary and secondary healthcare staff anywhere throughout England. SCR is extracted from GP held detailed medical records as a subset of clinical information or summary of medical information and is currently used in emergency and community pharmacy settings.

Apart from SCR, the other components of the NHS Care Records Service (NCRS) included, Personal Demographic Service (PDS), Secondary Uses Service (for various purposes including clinical research, clinical audit, management and commissioning), local Detailed Care Record (a locally held and locally available electronic record containing more detailed information than SCR) and previously existing paper or electronic records in GP surgeries, hospitals and other organisations. The delivery of SCR was supported by the NHS Spine (national infrastructure) through the Clinical Record Viewer (CRV) within England for shared use of authorised NHS staff and institutions. Several people raised their concerns about the security of the SCR and confidentiality of patient clinical information.

[56] Ibid.

[57] Mark Taylor and Natasha Taylor, 'Health Research Access To Personal Confidential Data In England And Wales: Assessing Any Gap In Public Attitude Between Preferable And Acceptable Models Of Consent' (2014)10 Life Science Society and Policy 15.

The **Care Record Guarantee** also described security tools to protect privacy and confidentiality of the patients including smartcards, recording permission to access, access controls, audit trails, further privacy controls and consent.[58] Following schematic diagram is adapted from (Cresswell & Sheikh 2009)[59] and recreated illustrating relationship of NHS SCR, Spine, CRS, DCR, HeathSpace, Choose & Book, ePrescription, PACS.

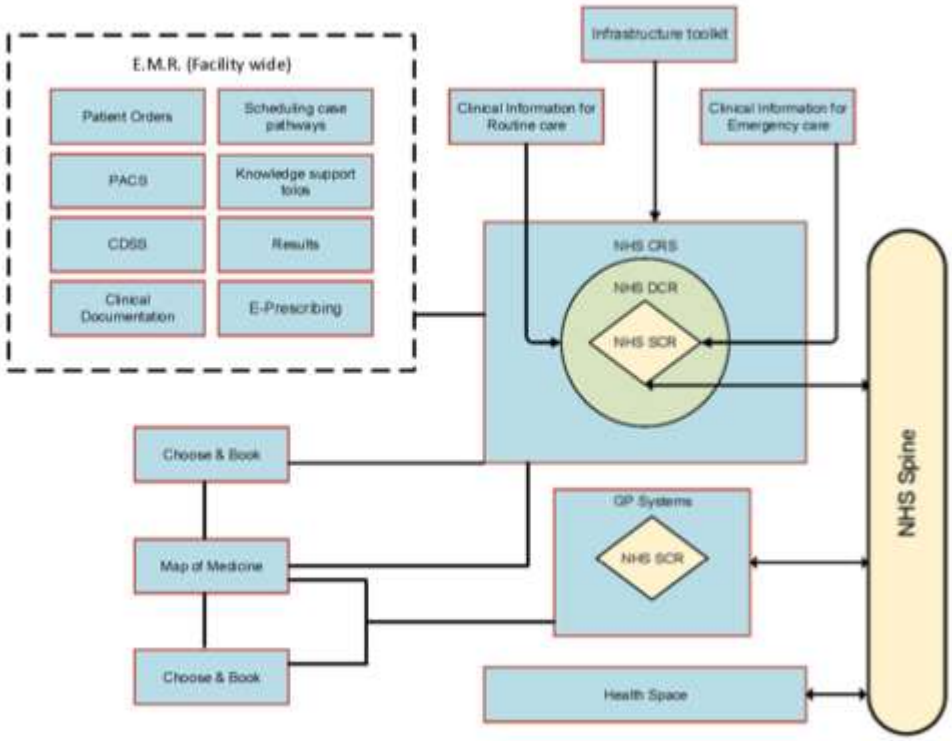


Figure 3.5. A schematic model of NHS SCR (Source: Cresswell & Sheikh 2009)

[58] ibid

[59] Kathrin Cresswell and Aziz Sheikh, 'The HNS Care Record Service (NHS CRS): Recommendations from the Literature on Successful Implementation and Adoption' (2009) 17(3) Informatics in Primary Care 153.

3.2.5. Care.Data

The care.data program was launched in 2013. It became controversial over security concerns and was scrapped in 2016.[60] The HSCIC extracts data from all different places where patients receive care, including GP surgery, hospital and community services; and shares for research through Care.Data Extraction Programme. By law, the GP surgeries are obliged to send patients' data to HSCIC for patients who have not opted out. The patients have two choices to opt out by preventing data from going to HSCIC (**a type 1 opt-out**) and by preventing HSCIC from passing out data to external third parties (**a type 2 opt-out**).[61] The care.data programme was paused in February 2014, after privacy groups arguments regarding lack of clarity in wording of the leaflets and leaflets not been distributed to all houses.[62] [63] The programme was restarted in autumn 2014 by six CCGs and it was found out in November 2015 that the type 2 opt-outs were not passed from GPs to the HSCIC, and the data from 700,000 patients who had opted out, was already shared by HSCIC.[64]

3.2.6. Caldicott 2

After growing perception that 'information governance' was an impediment to sharing of information even when sharing was thought to be in the best interest of the patient; in 2012 the 'NHS Future Forum' work stream on information, recommended a review to establish an appropriate balance between protection and sharing of patients' information to improve patient care. Government accepted the recommendation and subsequently Caldicott

[60] Matthew Limb, 'Controversial Database of Medical Records is Scrapped Over Security Concerns' (2016)354 BMJ i3804. <http://www.bmj.com/content/354/bmj.i3804> Accessed on 6 January 2017.
[61] House of Parliament, 'Electronic Health Records' (2015) Postnote 519
[62] Lizzie Presser, Maia Hruskova, Helen Rowbottom and others, 'Care.Data and Access to UK Health Records: Patient Privacy and Public Trust' (2015) Technology Science. <http://techscience.org/a/2015081103/> accessed on 15 January 2017.
[63] Sigrid Sterckx, Vojin Rakic, Julian Cockbain and others, 'You Hoped We Would Sleep Walk in to Accepting The Collection Of Our Data: Controversies Surrounding The UK Care.Data Scheme and Their Wider Relevance For Biomedical Research' (2016) 19(2) Med Health Care and Philos 177.
[64] House of Parliament (n 61)

2 review was published in March 2013. The 6 principles of '1997 Caldicott review' were updated. A 7th principle, "the duty to share information can be as important as the duty to protect patient confidentiality" was added and 26 recommendations were made. Government appointed Dame Fiona Caldicott as the first National Data Guardian (NDG) for health and care in November 2014.

3.3. Caldicott Review of Data Security, Consent and Opt-Outs (2016)

Dame Fiona Caldicott admitted in 'Review of Data Security, Consent and Opt-Outs' published in June 2016 that Caldicott2 review did not change public views very much on data sharing and opt-outs.[65] Several recommendations in this review made to the Department of Health and Government bodies include a new opt-out consent model and proposals for new data security standards in healthcare and social care along with a testing method for compliance against the standards. Recommendation is made to the Government for stronger sanctions including criminal penalties for deliberate and negligent re-identification of individuals to protect anonymised data. An eight-point model for consent and opt-out is presented in the review which includes that except for direct care, people can opt-out of sharing personal confidential data and people can still consent to the use of their confidential data in specific research projects even if opted out previously. A wide-range public consultation on the opt-out model proposals was recommended which has been completed by the Government in September 2016.

3.4. Care Quality Commission Review "Safe data, safe care"

The CQC has published a review 'Safe data, safe care' in July 2016 with six recommendations emphasising on data security, adequate staffing and technical support, internal and external audits and validation of new data security standards.[66]

[65] Department of Health. 'Review of Data Security, Consent and Opt-Outs'. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF> accessed on 4 December 2016).

[66] CQC, 'Safe data, safe care' (2016) <http://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf> accessed on 5 Dec 2016.

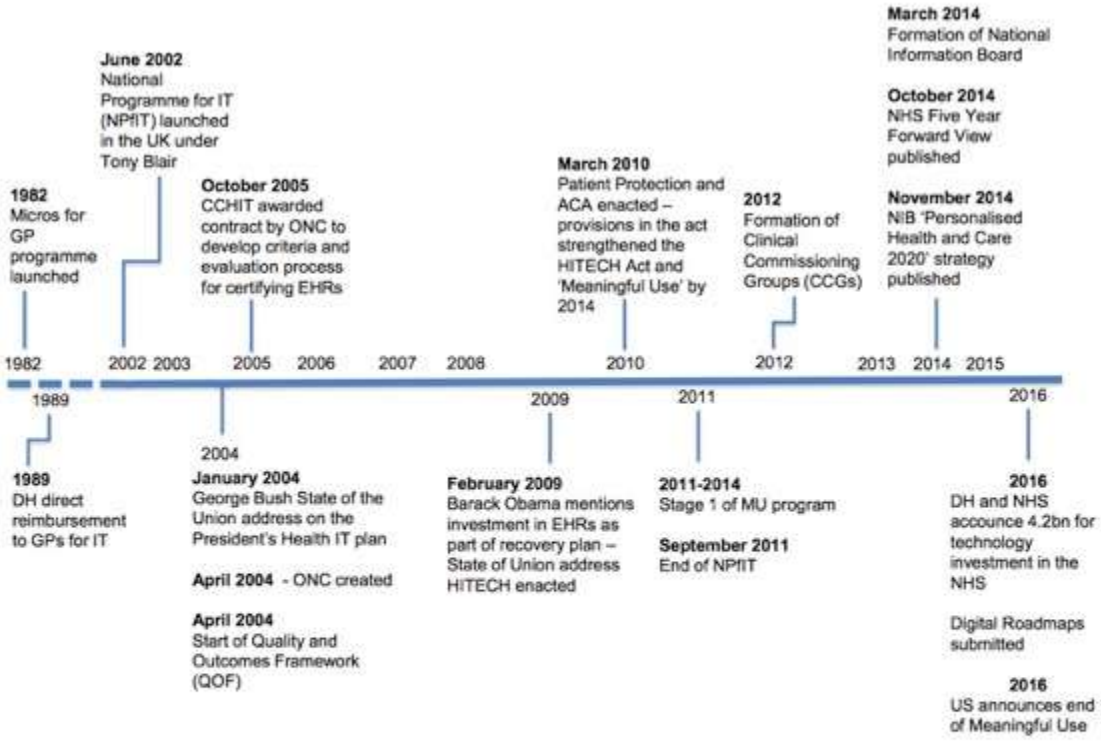
3.5. Wachter Review

Professor Robert Wachter and the advisory board published review in September 2016 and made 10 recommendations for further implementation of healthcare IT systems in England. The 6th finding in the report, 'While Privacy is Very Important, So Too is Data Sharing' states:

> Privacy is very important, but it is easy for privacy and confidentiality concerns to hinder data sharing that is desirable for patient care and research. Striking the right balance is critical. The problems with the implementation of the care.data programme – which lacked a comprehensive communication strategy to engage with the public and a clear protocol regarding who could access the data – illustrate how sensitive these issues are.
>
> Nevertheless, it would be a mistake to lock down everyone's healthcare data in the name of privacy. It is critical that appropriate technical safeguards are in place. It is equally critical to design and implement a system of regulation and governance that reassures patients that their rights and interests are fully respected, that provides clear guidance to professionals and managers, that effectively monitors for problems, and that takes actions where needed. The key is proportionate governance: balancing individual rights while recognising the enormous opportunities for patient benefit through the systematic secondary uses of NHS's unique national data assets. We endorse the recommendation of the National Data Guardian's 2016 Review of Data Security, Consent, and Opt-Outs, which was commissioned to achieve this balance.[67]

[67] Department of Health, National Advisory Group on Health Information Technology in England, 'Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England' (2016). <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550866/Wachter_Review_Accessible.pdf > accessed on 18 January 2017.

The following diagram shows the milestones in digitising the NHS.



* Includes relevant milestones in the US as well.

Abbreviations: GP, general practitioners; DH, UK Department of Health; IT, information technology; NPfIT, National Programme for Information Technology; CCHIT, Certification Commission for Health Information Technology (US); ONC, Office of the National Coordinator for Health Information Technology (US); QOF, Quality and Outcomes Framework; ACA, Affordable Care Act (US); HITECH, Health Information Technology for Economic and Clinical Health Act (US); MU, Meaningful Use (US); NHS, National Health Service; NIB, National Information Board.

Figure 3.6: 'Milestones in Digitising the NHS' (Source: Wachter Review 2016)[68]

[68] ibid

3.6. Summary

Multiple attempts were made to improve the quality of service by changing the structure of NHS but major NHS reforms in England took place after April 2013. The UK's largest public sector IT programme, NPfIT in NHS, was dismantled after 10 years in 2011 due to delays, escalating costs opposition of stakeholders and various implementation issues including criticism on top-down implementation policy. HSCIC (electronic health data warehouse), SCR, care.data, Caldicott's reviews, CQC & Wachter reviews discussed in this chapter provide basis for chapter 7 "secondary use of health data".

Chapter 4: EHR components, uses and standards

This chapter discusses uses, core components with their functionalities and standards of EHR.

4.1. Uses of Electronic Health Records

There are primary and secondary uses of EHR. The use of information or health record for its original purpose, such as patient care delivery, patient care management, patient care support processes, patient self-management, financial and other administrative processes is called a primary use.

The use or reuse of health record or patient health information's for different purposes, other than one for its acquisition is called a secondary use. IOM [69] described following primary and secondary uses of EHR.

Primary Uses

- Patient Care Delivery
- Patient Care Management
- Patient Care Support Processes
- Financial and other Administrative Processes
- Patient Self-Management

[69] NIH NCRR, 'Electronic Health Records Overview' 2006. <http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/Code%20180%20MITRE%20Key%20Components%20of%20an%20EHR.pdf> (accessed on 10 December 2016).

Secondary Uses

- Research
- Regulation
- Public Health
- Education
- National Security
- Policy Support

4.2. Core Components and Functions of EHR

The key components of an EHR include administrative, laboratory and radiology, pharmacy systems; computerised physician order entry, clinical documentation and decision support service (DSS). A general conceptual overview of Pre-EHR, EHR and future vision of EHR is shown in the following schematic diagram.

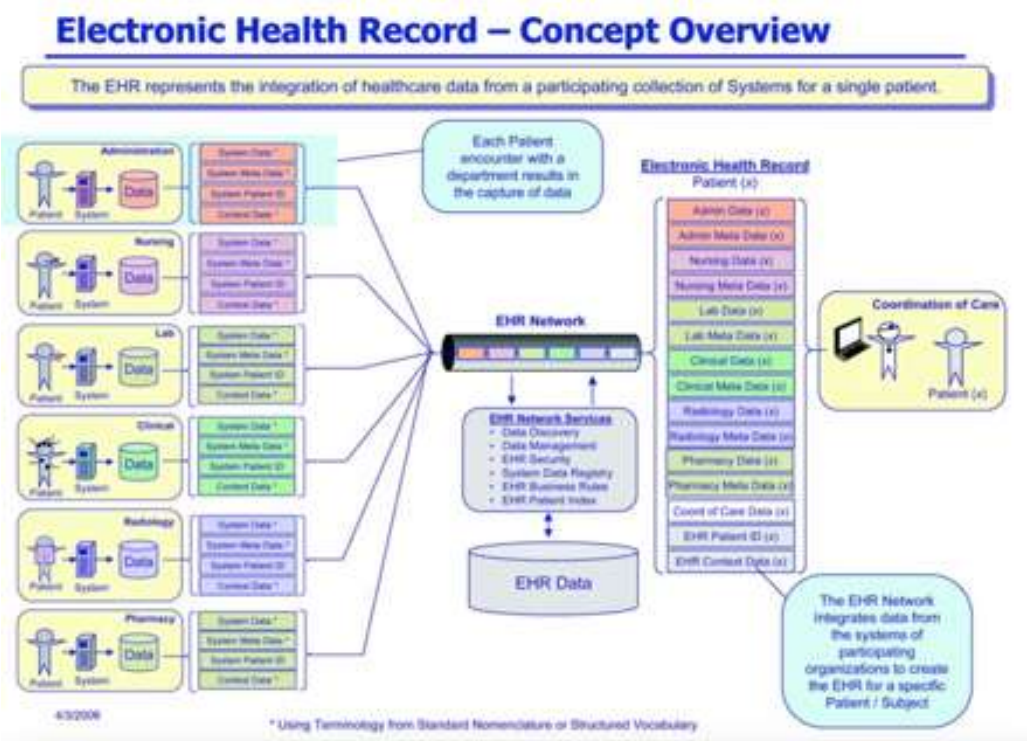


Figure 4.1 – EHR Concept Overview (Source NIH NCRR)[70]

[70] ibid

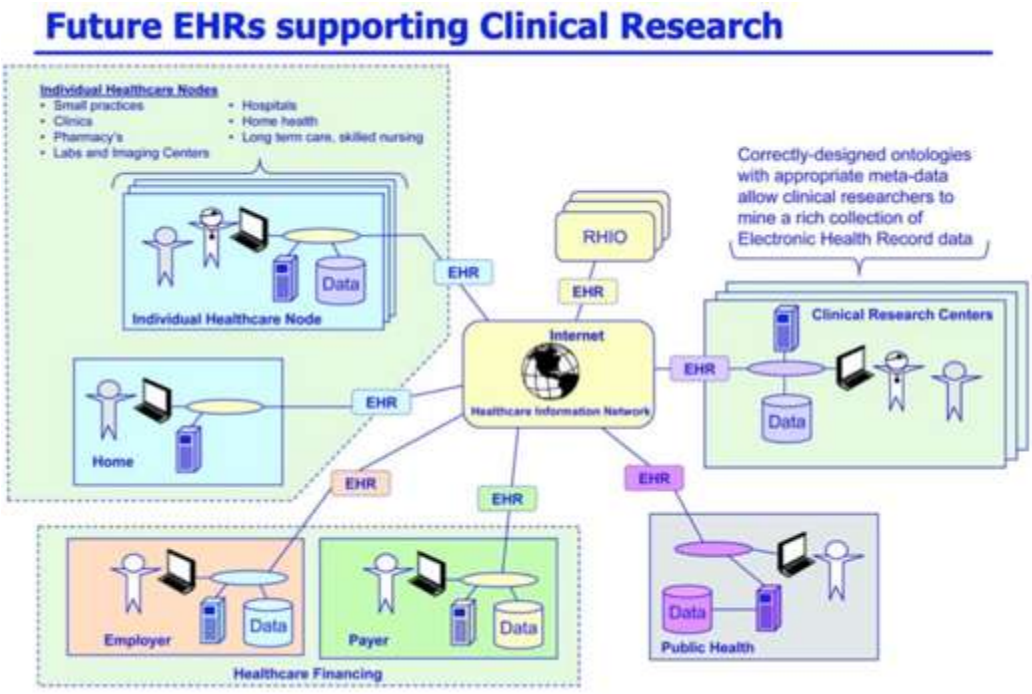


Figure 4.2: Future EHRs Supporting Clinical Research (Source NIH NCRR)[71]

In 2003 Institute of Medicine (IOM) identified eight core functionalities of an EHR system which include: health information and data, order entry/ management, results management, decision support, electronic communication and connectivity, patient support, administrative support, and reporting & population health management"[72]

4.2.1. Health Information and Data

Physicians need patients' information such as presenting complaints, laboratory and radiology test results, nursing entries (vital signs and so on) history of previous illness, surgery, medication and family history of disease to make an accurate diagnosis and treatment plans.[73] Medication errors can be

[71] ibid
[72] Institute of Medicine, 'Key Capabilities of an Electronic Health System: Letter Report' (2003) The National Academies Press.
[73] David Blumenthal and John Glaser, 'Information Technology Comes to Medicine' (2007)356(24) NEJM 2527.

reduced by the availability of patient information of allergies, reminders and medication alerts.[74] Capability of EHR to display all this information to the clinicians, when they need it, can reduce unnecessary tests, procedures and delay in the patient management.

4.2.2. Order Entry/ Management

Computerised physician order entry (CPOE) is an important component of EHR and a useful tool for patient safety and quality improvement as well as modernisation of the medical practice. CPOE is a process of computerised entry of instructions in to the medical record of a patient (such as orders for medication, laboratory and radiology) by an authorised healthcare professional under his or her care. In an EHR system, these orders are communicated to the relevant medical staff or departments for order completion over a computer network. Systems used by the physicians to enter orders can have significant effects on quality and costs of care [75,76,77,78,79] and proactively influencing physicians' orders can significantly affect patient

outcomes.[80,81] Computerised Provider Order Management (CPOM) and Computerised Provider Order Entry are sometimes used alternative terms for Computerised Physician Order Entry (CPOE).

[74] Gilad Kuperman and Richard Gibson, 'Computer physician order entry: Benefits, costs, and issues' (2003) 139 (1) Annals of International Medicine 31.
[75] G Octo Barnett, 'The application of computer-based medical-record systems in ambulatory practice' (1984) 310 New England Journal of Medicine 1643.
[76] William Tierney, Clement McDonald, Douglas Martin and others, 'Computerized Display of Past Test Results. Effect on Outpatient Testing' (1987) 107 Annals of Internal Medicine 569.
[77] William Tierney, Michael Miller and Clement McDonald, 'The Effect on Test Ordering of Informing Physicians of the Charges for Outpatient Diagnostic Tests' (1990) 322 New England Journal of Medicine 1499.
[78] William Tierney, Michael Miller, J. Marc Overhage and others,' Physician inpatient order writing on microcomputer workstations: Effects on resource utilization'(1993) 269 (3) Journal of the American Medical Association 379.
[79] Dean Sitting and William Stead, 'Computer-Based Physician Order Entry: The State-of-The-Art' (1994) 1 Journal of the American Medical Informatics Association 108.
[80] Clement McDonald, 'Protocol-Based Computer Reminders, The Quality of Care, and the Non-Perfectibility of Man' (1976) 295 New England Journal of Medicine 1351

4.2.3. Results Management

There are several advantages of computerised test results over paper-based test results (for example radiology procedure result reports and images, laboratory test results and so on). Computerised results can be communicated and accessed more easily and rapidly, making available to the care providers at the time and place where they are needed, for quicker diagnosis and treatment enhancing efficiency and quality of care.[82] Other advantages of computerised test results include automated display of previous test results economising redundancy and costs [83,84,85]; easier visualization of abnormalities as well as better interpretation ensuring appropriate follow-up [86,87,88], and improved care coordination among multiple care providers due to access to electronic consultations and patient consents[89].

4.2.4. Clinical Decision Support (CDS)

CDS system is a health information technology system designed to assist healthcare professionals for clinical decision making by providing intelligently filtered knowledge, based on patient-specific information, to enhance healthcare. Several studies have shown effectiveness of CDS in enhancing clinical performance for several aspects of healthcare which include

[81] Clement McDonald, Siu Hui, David Smith and others, 'Reminders to Physicians from an Introspective Computer Medical Record: A Two-Year Randomised Trial' (1984) 100 Annals of Internal Medicine 130.
[82] David Bates and Atul Gawande, 'Improving Safety with Information Technology' 2003; 348(25) NEJM 2526.
[83] ibid
[84] Steven Shea, Justin Starren, Ruth Weinstock, and others D , 'Columbia University's Informatics For Diabetes Education And Telemedicine (Ideatel) Project: Rationale And Design' (2002) 9 (1)J Am Med Inform Assoc 49.
[85] William Tierney, Clement McDonald, Douglas Martin and others, 'Computerized Display of Past Test Results. Effect on Outpatient Testing' (1987) 107 Annals of Internal Medicine 569.
[86] J. Marc Overhage, Jeffrey Suico and Clement Mc Donald, 'Electronic Laboratory Reporting: Barriers, Solutions and Findings' (2001) 7 (6) J Public Health Manag Pract 60.
[87] Gordon Schiff, David Klass, Josh Peterson, and others, 'Linking Laboratory and Pharmacy: Opportunities for Reducing Errors And Improving Care' (1993)163 (8) Arch Intern Med 893.
[88] David Bates (n 82).
[89] ibid

preventive care, disease outbreaks, diagnosis and therapeutic management, drug prescription and adverse events detection. [90,91,92] There are several issues related to the design, implementation and legal aspects of CDS.[93]

4.2.5. Electronic Communication and Connectivity

Electronic communication tools can enhance coordination of care, effective disease management, patient safety and quality of care by timely and efficient communication among healthcare professionals and with patients whereas lack of communication can contribute to the occurrence of adverse events.[94,95,96,97] Patients' can view their summary data from EHR (for example results of diagnostic tests), request renewal of a prescription, scheduling of an appointment, medical advice or update their demographic information through eHealth applications with a secure access to their EHR.[98] The EHR systems' capability to send, automated notification messages to the ordering physicians via message centre as alerts on their computers, or emails or text messages to their mobile devices for critical laboratory or radiology results has been shown to be an effective communication among providers and with

[90] ibid

[91] Dereck Hunt, R. Brian Haynes, Steven Hanna and others, 'Effects of Computer-Based Clinical Decision Support Systems on Physician Performance and Patient Outcomes: A Systematic Review' (1998) 280 (15) JAMA 1339

[92] Mary Johnston, Karl Langton, R. Brian Haynes, and others, 'Effects of Computer-Based Clinical Support Systems on Clinician Performance and Patient Outcome. A Clinical Appraisal of Research' (1994) 120 (2) Am Intern Med 135.

[93] HIMSS, 'CDS: Fundamental Issues' < http://www.himss.org/library/clinical-decision-support/issues?navItemNumber=13240 > accessed on 9 December 2016

[94] David Bates (n 82).

[95] Laura Peterson, Troyen Brennan, Anne O'Neil, and , 'Does House Staff Discontinuity of Care Increase the Risk for Preventable Adverse Events?' (1994)121 (11) Ann Intern Med 866.

[96] Ingrid Schmidt and Bonnie Svarstad, 'Nurse-Physician Communication and Quality of Drug Use in Swedish Nursing Homes' (2002) 54 (12) Soc Sci Med 1767.

[97] Richard Wanlass, Sandra Reutter and Anthony Kline, 'Communication Among Rehabilitation Staff: "Mild", "Moderate" or "Severe" Deficits?' (1992)73(5) Arch Phys Med Rehabil 477.

[98] Paul Tang, William Black, Jenny Buchanan, and others. . PAMFOnline, 'Integrating EHealth with an Electronic Medical Record System' AMIA Annual Symposium Proceedings. 2003, 644-648. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1479999/ >accessed on 10 December 2016.

patients[99,100,101] ; whereas some studies have mixed results.[102] There are potential privacy risks when the messages can get misdirected or the mobile devices become accessible to unauthorised users.[103]

4.2.6. Patient Support

EHR provides tools for patients' access to the educational materials, their health records and facilitate them to perform self-testing and carry-out home-monitoring, which can significantly improve control of chronic conditions,[104] especially interactive education has shown positive results in diabetes.[105]

4.2.7. Administrative Processes

The administrative process includes patients' registration (obtaining demographic information, information of insurance plan or financial responsibility for billing purposes), eligibility check (verification of insurance cover or willingness to accept full financial responsibility for the services), scheduling for appointment, check-in for scheduled visit, clinical encounter (usually a nurse or a medical assistant first obtains vitals, blood and urine samples if required, and updates subjective history of the patient; the physician examines the patient; updates the clinical notes in SOAP order –

[99] E. Andrew Balas, Farah Jaffrey, Gilad Kuperman, and others, 'Electronic Communication with Patients. Evaluation of Distance Medicine Technology' (1997) 278 (2) JAMA 152.

[100] Eric Liederman and Catrina Morefield, 'Web Messaging: A New Tool for Patient-Physician Communication' (2003)10 (3) J Am Med Inform Assoc 260.

[101] Eugene Worth and Timothy Patrick, 'Do Electronic Mail Discussion Lists Act as Virtual Colleagues?' (1997) Proc AMIA Annu Fall Symp 325.

[102] Edward Liebow, James Derzon, John Fontanesi, and others, 'Effectiveness of Automated Notification and Customer Service Call Centres for Timely and Accurate Reporting of Critical Values: A Laboratory Medicine Best Practices Systematic Review and Meta-Analysis' (2012) 45 (0) Clinical biochemistry 979.

[103] ibid

[104] Scott Weingarten, James Henning, Enkhe Badamgarak, and others, 'Interventions Used in Disease Management Programmes for Patients With Chronic Illness- Which Ones Work? Meta-Analysis of Published Reports'(2002) 325 (7370) BMJ 925.

[105] Santosh Krishna, E Andrew Balas, Donal Spencer, and others, 'Clincal Trials of Interactive Computerised Patient Education: Implications For Family Practice' (1997) 45 (1) J Fam Prac 25.

abbreviated from subjective, objective, assessment and plan), check-out (the patient is discharged after receptionist schedules any follow-up visit and billing formalities are completed).[106] A typical outpatient workflow is shown in the following diagram.

Figure 4.3: Outpatient workflow diagram. (Source: Health Informatics, Robert Hoyt)[107]

In the UK, the Patient Administration System (PAS) was being widely used in NHS for long time even before NPfIT project with core functions including mater patient index, appointment booking, waiting list management, record of patient activity, activity returns/ billing, reporting and admissions.

The electronic scheduling systems for outpatient and inpatient procedures, patient visits and hospital admissions increase efficacy of health care organizations as well as provide more timely service to the patients.[108,109,110]

[106] Rober Hoyt & Ann Yoshihashi, *Health Informatics: Practical Guide for Healthcare and Information Technology Professionals*. (6th edn, Pensacola, Fl. Lulu.com 2014).
[107] ibid.
[108] Jeffrey Everett, 'A Decision Support Simulation Model for the Management of an Elective Surgery Waiting System' (2002) 5 (2): Health Care Manag Sci 89.
[109] Walton Hancock, and Paul Walter. 1986. Reduce Hospital Costs With Admissions and Operating Room Scheduling Systems. Softw Healthc 4 (1):42-6.

4.2.8. Reporting and Population Health Management

Immunization status and bio-surveillance data reports can be generated in an electronic format and tracked which improves speed and accuracy of such data. The clinical dashboards can be made for clinicians for routine reporting of key quality indicators to improve quality of the services.

4.3. Standards of EHR

'A standard comprises a set of rules and definitions that specify how to carry out a process or produce a product.'[111] In 'Handbook of Medical Informatics', Bemmel and Musen stated that, a 'standard' is 'established by consensus and approved by a recognized body that provides rules, guidelines, or characteristics for activities.'[112]

The Royal College of Physicians prepared a document 'Standards for the clinical structure and content of patient records' on behalf of the HSCIC and was signed off by the Academy of Medical Royal Colleges in April 2013 as 'fit for purpose' for the whole medical profession.[113] It describes standards for the structure and content of patient records, inpatient clerking, handover communications, discharge summaries, referral letters and outpatient letters.

The Department of Health Code of Practice, 'Records Management Code of Practice for Health and Social Care 2016' demands that the Code must be read in conjunction with the 'standards document' of the Academy of Medical Royal Colleges.

[110] Lauren Woods. 2001. What Works: Scheduling. Picture Perfect Solution. The Right Technology and an ASP Solution Bring Scheduling Efficiency and Added Revenue to a Community Hospital's Radiology Department. Health Manag Technol 22 (8):48-50.
[111] Edwad Shortliffe and James Cimino. 3rd ed., Biomedical Informatics, Springer, New York. 2006.
[112] Bemmel and Musen (n 17) para 597.
[113] HSCIC, Academy of Medical Royal Colleges (n 19).

4.4. Summary

This core components of an EHR include administrative, laboratory and radiology, pharmacy systems; CPOE, clinical documentation and DSS. The functionalities of key components, uses and standards of EHR are discussed along with literature review.

Chapter 5: Advantages of EHR

The potential benefits of EHR can be divided in to three categories based on outcomes that include clinical outcomes (for example reduced medical errors, improved quality of care), organizational outcomes (for example operational and financial benefits) and societal outcomes (for example improved population health, improved ability to carry out research, reduced costs).[114]

5.1. Clinical outcomes

The degree of increase in likelihood of desired health outcomes, consistent with current professional knowledge, indicates quality of health care.[115] Among the measureable indicators of quality health care, including (5Ds) death, disease, disability, discomfort, and dissatisfaction[116] and conceptual components of quality health care, including safe, effective, patient centred, timely, efficient, and equitable; safety is the key element and foundation component of quality.[117]

Safety in health care means 'avoiding injuries to patients from the care that is intended to help them'.[118] The 21st century health care delivery systems adopt six conceptual components of the quality health care.[119] Studies have shown that for hospital patients computerised physician reminders increased the use of influenza and pneumococcal vaccinations from 0% to 35% and 50% respectively.[120] Comparable results were found on vaccination rates in other

[114] Nir Menachemi, Taleah , 'Benefits And Drawbacks Of Electronic Health Record Systems' (2011) 4:47 Risk Management and Healthcare Policy 55
[115] Kathleen Lohr, Steven Schroeder, 'A Strategy for Quality Assurance in Medicine' (1990) 322 NEJM 1161.
[116] Kathleen Lohr, 'Outcome Measurements: Concepts and Questions' (1988) 25(1) Inquiry 37.
[117] IOM Committee on the Quality of Health Care in America, '*Crossing the quality chasm: A new health system for the 21st century*, (2001) National Academy Press.
[118] Ibid.
[119] Ibid.
[120] Paul Dexter, Susan Perkins, J. Mark Overhage, and others, 'A computerized reminder system to increase the use of preventive care for hospitalized patient' (2001 345 (3) NEJM 965.

studies showing that computerised reminders can improve adherence to guidelines for immunization.[121] [,122] A study showed that computer alerts increased 19% prophylactic use of anticoagulation, which resulted in a 41% reduced risk of deep vein thrombosis (DVT) or pulmonary embolism (PE) at 90 days' post discharge.[123] Some other studies have shown, a 55% reduction in serious medication errors linked with CPOE system usage in the hospital setting and further medication error reduction up to 86% by adding CDS system to a CPOE system.[124,125]

5.2. Organizational outcomes

The organizational outcomes related to EHR include increase in revenue, cost reduction, improvement in regulatory and legal compliance, improvement in ability to conduct research, and increase in job satisfaction among physicians.[126] Reduced billing errors, improved charge capture, and improved cash flow can increase revenue.[127]

EHR's role in, reduction or elimination of billing or coding errors[128,129,130] and increased patient visits due to reminders to the patients and providers about

[121] Clement McDonald, Siu Hui and William Tierney, 'Effects of Computer Reminders for Influenza Vaccination on Morbidity During Influenza Epidemics' (1992)9(5) MD Comput 304.
[122] William Tierney, Siu Hui and Clement McDonald, 'Delayed Feedback of Physician Performance Versus Immediate Reminders to Perform Preventive Care. Effects on Physician Compliance' (1986) 24(8) Med Care 659.
[123] Nils Kucher, Sophia Koo, Rene Quiroz, and others, 'Electronic Alerts to Prevent Venous Thromboembolism Among Hospitalized Patients' (2005)352(10) NEJM 969.
[124] David Bates, Lucain Leape, David Cullen, and others, 'Effect of Computerized Physician Order Entry and a Team Intervention on Prevention of Serious Medication Errors' (1998)280(15) JAMA 1311.
[125] David Bates, Jonathan Teich, Joshua Lee , and others,'The Impact of Computerized Physician Order Entry on Medication Error Prevention' (1999)6(4) J Am Med Inform Assoc 313.
[126] Menachemi (n 114)
[127] ibid.
[128] Tricia Erstad, 'Analyzing computer based patient records: a review of literature' (2003) 17(4) J Healthc Inf Manag 51.
[129] Abha Agrawal, 'Return on Investment Analysis for a Computer-Based Patient Record in the Outpatient Clinic Setting' (2002) 13(3) J Assoc Acad Minor Phys 61.
[130] Jemma Mildon, Trevor Cohen, 'Drivers in The Electronic Medical Records Market' (2001) 22 Health Manag Technol 14.

routine health check-ups[131] has been studied and proved to be cause of enhanced revenue.

EHR's use reduces redundant diagnostic test usage or need to send diagnostic test results hard copies to different providers through mail.[132,133] The patient information becomes more readily available with EHR use as compared to paper records, which reduces costs related to chart pulls[134] and supplies needed for paper charts[135]. Other studies have shown that EHR use is associated with higher operational performance[136] and improved legal and regulatory compliance[137].

5.3. Societal benefits

The EHR has ability to facilitate research by gathering data and conducting studies more easily and economically.[138] It is expected that increase in adoption of EHR will grow the pool of electronically stored data.

5.4. Summary

The benefits of EHR are described in three broad categories based on outcomes. The benefits include reduced medical errors; improvement in quality of care, population health, ability to carry out research, reduced costs, and operational and financial benefits.

---

[131] ibid

[132] Phillip Chen, Milenko Tanasijevic, Ronald Schoenenberger, and others, 'A Computer-Based Intervention for Improving the Appropriateness of Antiepileptic Drug Level Monitoring' (2003) Am J Clin Pathol 432.

[133] Tierney (n 78).

[134] Samuel Wang, Blackford Middleton, Lisa Prosser, and others, 'A Cost-Benefit Analysis of Electronic Medical Records in Primary Care' [2003] (5) Am J Med 397, 114.

[135] Tom Ewing, Doug Cusick, 'Knowing what to measure' (2004) 58(6) Healthcare Financial Management 60.

[136] Anol Bhattacherjee , Neset Hikmet, Nir Menachemi, and others. The differential performance effects of healthcare information technology adoption. Information Systems Management. 2007; 24(1):5-14.

[137] Agrawal (n 129).

[138] John Powell and Ian Buchan, 'Electronic Health Records Should Support Clinical Research' Journal of Medical Internet Research. 2005; 7(1): e4. <https://www.jmir.org/2005/1/e4/ >accessed on 16 January 2017.

Chapter 6: Disadvantages of EHR

The potential drawbacks of EHR include financial challenges, privacy and security issues.

6.1. Financial issues

The initial costs for EHR adoption include hardware, software and training costs, and costs related to conversion of existing paper records to electronic records. Other costs include maintenance, software and hardware upgradation and replacement costs. Implementation of EHR can also cause temporary decline in revenue due to reduced productivity. Although the initial costs of hardware and software installation are dropping due to rapidly advancing information technology, but these upfront costs are still high for relatively smaller practices and is one of the major barriers to implementation of EHR.[139] Some studies have shown that there was initial reduced productivity and loss of revenue after implementation of EHR due to training and learning of the end-user staff.[140]

6.2. Ethical and legal issues

The ethical and legal ramifications of EHR can be addressed through ethical principles and legal framework. The ethical fundamentals are described briefly prior to the discussion of ethical and legal challenges of EHR.

6.2.1. Ethical fundamentals and ethical frameworks

Application of ethical principles such as autonomy, beneficence, non-maleficence, and justice can address the ethical ramifications of EHR. This section provides a brief description of fundamentals of ethics, definitions and ethical frameworks to approach ethical challenges of EHR.

[139] Menachemi (n 114)

[140] Neil Fleming, Steven Culler, Russell McCorkle, and others, 'The Financial and Nonfinancial Costs of Implementing Electronic Health Records in Primary Care Practices' (2011) 30(3) Health Aff (Millwood) 481.

The ethics can be described as 'a theory of right action and the greater good'; or 'principles that allow us to make decisions about right and wrong'; and the practice of these right actions and greater good is called morals.[141]

The categories of ethics include **normative or prescriptive ethics** (concerned with how should people act, what is good or bad and what is right or wrong – tries to establish a set of norms for action or a set of rules governing human conduct; it has three main categories – consequentialism, deontology and virtue ethic), **descriptive ethics** (what do people think is right – a study of peoples beliefs about morality), **meta-ethics** (what does 'right' mean – concerned with meaning of ethical judgements), and **applied ethics** (application of ethical theory or moral principles and judgements to real-life situation).[142]

A branch of applied ethics, which deals with resolving difficult and controversial ethical questions that arise from the practice of medicine is called **medical ethics**; whereas, the term '**bioethics**' has more broader scope than the scope of traditional medical ethics and embraces philosophy of science and issues of biotechnology.[143] The medical ethics can be considered a sub-discipline of bioethics along with other sub-disciplines of bioethics including animal ethics and environmental ethics. Schaller described bioethics as 'a discipline concerned with studying and resolving life-changing biomedical problems using ethical principles.'[144]

The (bio)ethical theories include:

[141] Luke Mastin, 'The Basics of Philosophy' <http://www.philosophybasics.com/branch_ethics.html#Introduction> accessed on 30 December 2016.
[142] Ibid.
[143] Emily Jackson, '*Medical law: text, cases, and materials*' (2nd edn, OUP 2010).
[144] Barry Schaller, *Understanding Bioethics and the Law: The Promises and Perils of the Brave New World of Biotechnology* (Praeger 2008)

i. **deontological** approach (applies usually strict moral rules or norms to concrete cases – an action is considered morally right or wrong because of the characteristics of action itself; not because of the consequences of the action or because of the character and habits of the actor),

ii. **utilitarianism** (a type of consequentialism, which holds that an action is right if it leads to the greatest happiness or pleasure for the greater number of people - core elements include consequence principle, utility principle, hedonistic principle and universal principle),

iii. **principlism** (4 principles – a more practical approach to decide medical issue),

iv. **virtue ethics** (one should act in accordance with what the virtuous person would have chosen – focuses on character instead of rules or consequences),

v. **casuistry** (case-based – a bottom-up approach instead of starting with general and broad rules) and

vi. **feminist** bioethics (particularistic by nature; a strong focus on care, rejecting the dominant emphasis upon patient autonomy; claims for an equal and just treatment of women, and values relationships more highly – relational autonomy).[145]

Beauchamp and Childress have described an approach to analyse and decide medical questions based on four prima facie moral principles. These four basic principles are: **autonomy** (the obligation to respect individual's self-governance; or the duty to respect the decision making capacities of autonomous persons; to enable individuals for making reasoned informed choices); **non-maleficence** (the duty to avoid causing harm); **beneficence** (the duty to do good; or provide benefits and to balance benefits against risks; or obligation to act in the best interest of the patient), and **justice** (the duty of fairness in the distribution of benefits against risks; or obligation to treat like cases alike and distribute scarce

[145] Mastin (n 141).

health resources fairly).[146] The four principles is one of the most widely used ethical frameworks, provides broad consideration of medical problems and is more practical ethical framework to decide medical issues. Other ethical frameworks to approach ethical problems in patient care include the four-quadrant approach[147] and CARE (Schneider and Snell 2000).[148]

Mark Rothstein stated that:

> Law and bioethics have similar – but not identical – aims. In matters such as privacy, conflicts of interest, and respect for persons, the law usually sets minimum standards of what *must* be done. By contrast, codes of ethics of health professionals and scholarship in bioethics generally set loftier goals of what *ought* to be done. [149]

Although most of the methods differ in approach to analyse ethical dilemmas, but result in almost similar conclusions when combined with best practice guidance and awareness of the law.

6.2.2. Ethical dilemmas of EHR

The patient privacy violation risk associated with EHR is an increasing concern for patients.[150] The EHR systems and providers are expected to maintain respect for patient autonomy and the patients should have a say in for decisions about the content, access, use and ownership of their health records. The unauthorized access, disclosure and secondary use without their knowledge or against their desire, will be violation of the ethical principle of autonomy.

[146] Tom Beauchamp and James Childress, *Principles of Biomedical Ethics* (1st edn, OUP 1979).
[147] Alber Jonsen , Mark Siegler , William Winslade, *Clinical ethics* (6th edn, McGraw-Hill 2006).
[148] Gregory Schneider and Laura Snell, 'CARE: An Approach for Teaching Ethics in Medicine' (2000) 51 Social Science and Medicine 1563.
[149] Mark Rothstein, 'The Role of Law in The Development of American Bioethics' (2009) 20 (4) J Int Bioethique 73.
[150] Laura Zurita, Christian Nohr, 'Patient Opinion: EHR Assessment from the Users' Perspective' (2004) 107(2) Stud Health Technol Inform 1333.

The 'autonomous patients' would expect to have access to their health records and many of them might desire to have a level of control over the content of their personal information[151], which is technically possible. On the other hand, it can be argued that by allowing patients to alter or delete their health records would conflict with the medical and legal utility of the health record. Therefore, the access can be limited, to view or challenge the health record, not to modify or delete the content entered by the health care professionals.[152]

The question of ownership of the EHR is an ethical issue that needs to be addressed. The autonomous patients can argue that the information in their health records belongs to them and they are the owners just like their money in their bank accounts remains their property. Banks can manage their bank accounts but cannot become owner of their money. The providers and vendors of EHR can argue that they create the EHR software, health records and maintain data storage server, therefore, they are the owners of information. These ethical questions about the ownership of patients' health information have already been raised,[153] and ethical as well as legal early rectification of these conflicts between patient and professional autonomy, economic and personal value, and business interests is required.[154]

In February 2014, NHS sold 47 million electronic medical records to the insurance companies. [155,156] The data included medical histories of inpatients

[151] Kenneth Mandl, Peter Szolovits, Isaac Kohane, 'Public Standards And Patients Control: How To Keep Electronic Medical Records Accessible But Private' (2001)322(7281) BMJ 283.
[152] Ibid.
[153] Marc Rodwin, 'The Case for Public Ownership of Patient Data' (2009)302(1) JAMA 86.
[154] Mark Hall, Kevin Schulman, 'Ownership of Medical Information' (2009)301(12) JAMA 1282.
[155] Laura Donnelly, 'Britain's National Health Service: Medical Records Database "Raises Serious Privacy Issues — Patients deliberately kept in the dark"' Johnib Wordpress (17 February 2014) <https://johnib.wordpress.com/2014/02/17/britains-national-health-service-medical-records-database-raises-serious-privacy-issues-patients-deliberately-kept-in-the-dark/> accessed November 10, 2016.

from 1997 to 2010 in the UK. As the de-identified data, can be re-identified with the help of external data sources[157], voices of right to opt out from EHR were raised by the patient advocacy groups.[158]

The identification of the patient information can harm the patient's dignity and is against the ethical principle of non-maleficence (duty to avoid harm). On the other hand, there is great potential to conduct clinical and biomedical research by using EHR data that will benefit to the individual patients as well as to the whole society. The ethical principle of beneficence (duty to do good) justifies clinical research but conflicts with the ethical principle of non-maleficence if the health information of the patient becomes public. A utilitarian approach would be to weigh the harm to the individual or a group of individuals because of violation of privacy due to re-identification of data against the potential benefit to the society from the research and if the benefits of research outweigh risk of harm to the individual or group or individuals, and it led to health benefits for the whole society, it might be justifiable to the utilitarian. However, if the possible benefits to the population are marginal, a utilitarian might reach a different conclusion. On the other hand, a Kantian would be concerned with the rights and interests of the individual or group of individuals. A Kantian's (deontological) approach would be whether autonomy of the individual or group of individuals has been respected. A Kantian might accept the research if the individual or the group was properly consented for use of the data for that research and the research was also going to benefit the subject.

Choice of opting out is another ethical dilemma as the patient who opt out from EHR, might be at disadvantage of not getting better quality healthcare

[156] Steven Swinford, 'Britain Considers Law To Protect Medical Records, Patient Data After National Service Sold Info To Insurers' Johnib Wordpress, <http://johnib.wordpress.com/2014/03/01/britain-considers-law-to-protect-medical-records-patient-data-after-national-health-service-sold-info-to-insurers/> (accessed November 10, 2016).
[157] Latanya Sweeney, 'A Model for Protecting Privacy' (2002)10(5) IJUFKS 557.
[158] Michael Day, 'Patients Can Opt Out of Controversial National Records System' (2007)334(7583) BMJ 12.

service. This will not only be unfair to the patient as it will be against the ethical principle of justice (the duty of fairness in the distribution of benefits against risks), but will also affect the quality of the clinical research. More research is required to find solutions that can satisfy the protection of patients' information as well as conduction of research by utilising EHR 'quality' data.

Some patient groups might not have enough technical skills or financial resources to avail the full benefits of EHR that will create new injustices in the society. There is pre-existing technology gap among different socioeconomic groups created by the digital divide; due to availability of greater sophisticated computers, level of internet access and usage to the higher socioeconomic status groups[159] that can be exacerbated by the EHR systems, as the lower socioeconomic status patients may have reduced access to the accessible EHR systems.

Integrity of the EHR data is vital to provide safe and quality care to the patient. Inaccurate data entries have been reported because of 'cut and paste' options available to the health care professionals raising concerns about the integrity and reliability of the clinical data.[160] This practice can harm the patient that will be against the ethical principle.

6.2.3. Legal dilemmas of EHR

The common law, the HRA 1998, the DPA 1998 and other legislation govern the privacy of patients' identifiable data. The NHS confidentiality Code of Practice, GMC guidance and the Caldicott Principles describe confidentiality requirements from health care professionals. In the UK, the health care professionals under the DPA 1998 are required to obtain a patient's consent to store information about them to provide health care and stating the purpose

[159] Emily Kontos, Gary Bennett, Kasisomayajula Viswanath, 'Benefits And Facilities to Home Computer and Internet Use Among Urban Novice Computer Users of Low Socioeconomic Position' (2009)9(4) J Med Internet Re e31 <http://www.jmir.org/2007/4/e31/> accessed on 1 January 2017.

[160] Robert Hirschtick, 'A piece of my mind. Copy-and-paste' (2006) JAMA 295.

for which the information is being stored. In situations where allegations of negligence are made, records of patient care and treatment have important role in providing evidence of appropriate patient care. The secondary uses of EHR and topics of privacy, confidentiality and consent are discussed in detail in the next chapter.

The EHR systems may increase legal responsibility and accountability of health care professionals.[161] The other EHR related issues include, responsibilities of healthcare professionals reviewing the entire clinical summary from multiple clinicians and institutions accessible through computers; the liabilities resulting from overriding alerts and warnings from clinical decision support (CDS); physicians' rights to uninterrupted EHR access, right to see all data required to provide safe and effective care, right to a succinct patient summary and right to override computer-generated alerts.

6.3. Security

Security refers to the measures used to safeguard information. The security of the patient data refers to the access to the confidential information controlled and managed by the technical and procedural methods with the aim to protect and safe guard from unauthorized or unintentional access, modification, disclosure, or destruction.

Confidentiality, integrity and availability are three basic goals of security. [162,163] Confidentiality ensures accessibility of information only to the authorized user.[164] Integrity ensures accuracy of that information without any modification in an unauthorised way. Availability ensures accessibility and usability of that

[161] Sandeep Mangalmurti, Lindsey Murtagh, Michelle Mello M, 'Medical Malpractice Liability in the Age of Electronic Health Records.' (2010) 363 (21) NEJM 2060.
[162] Sebastian Haas, Sven Wohlgemuth, Isao Echizen, and others, 'Aspects of Privacy for Electronic Health Records' (2011) 80(2) Int J Med Inform e26-e31. <http://www.sciencedirect.com/science/article/pii/S1532046412001864> accessed on 2 January 2017.
[163] Ross Anderson, 'Information Technology in Medical Practice: Safety and Privacy Lessons From The United Kingdom' (1999) 170 (14) Medical Journal of Australia 181.
[164] ISO/EN 13606.< http://www.iso.org/iso/home.htm/ > (accessed on 2 January 2017).

information by the authorised user when it is needed. To achieve these goals, several types of safeguards are required that include: administrative safeguards (actions, policies and procedures to prevent, detect, contain, and correct security violations),[165] physical safeguards (physical and technological measures, policies, and procedures to protect EHR systems, equipment and related buildings from unauthorized access, natural, and environmental hazards),[166] organizational standards,[167] and policies and procedures (creation and maintenance of written security policies and procedures as well as written records of required actions, activities and assessments with periodical reviewing and updating according to environmental or organizational requirements)[168]. Although most of the EHR systems come with inbuilt security features from vendors, but these might not be adequately configured or properly enabled. Therefore, it is responsibility of the care providers to implement all the necessary safeguards to protect the confidentiality, integrity and availability of the data in EHR.

6.4. Security threats to EHR and security measures

Several reports of theft or accidental loss of patients' sensitive clinical information in recent years[169,170,171,172,173] are serious data security and

[165] HIPAA, 'Summary of the HIPAA Security Rule' <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> (accessed on 2 January 2017).
[166] ibid
[167] ibid
[168] ibid.
[169] David Blumenthal, 'Wiring the Health System – Origins and Provisions of a New Federal Program' (2011) 365(24) N Engl J Med 2323.
[170] US Department of Health and Human Services Office for Civil Rights, 'Breaches affecting 500 or individuals' <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf> (Accessed on 3 January 2017).
[171] Big Brother Watch, 'NHS Breaches of Data Protection Law', (2001) <https://www.bigbrotherwatch.org.uk/files/NHS_Breaches_Data_Protection.pdf >Accessed on 3 January 2017.
[172] Big Brother Watch, 'NHS Data Breaches', (2014) <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/11/EMBARGO-0001-FRIDAY-14-NOVEMBER-BBW-NHS-Data-Breaches-Report.pdf> Accessed on 3 January 2017
[173] Vincent Liu, Mark Musen and Timothy Chou. 'Data Breaches of Protected Health Information in the United States' (2015)313(14) JAMA 1471.

privacy risks linked with EHR. Liu et al[174] reported 949 breaches affecting 29 million records between 2010 and 2013 in US. In this study, 11 percent of the breaches were due to accidental loss or improper disposal of data, whereas, the number of breaches increased from 12 percent to 27 percent during those three years due to hacking or unauthorized access.

The security threats to EHR systems can be from inside the organization or from outside that may be due to innocent mistakes resulting in accidental disclosures, abuse of access privileges, access information for personal gains, unauthorized physical intruders, and attacks from resentful employees or outsiders. EHR systems are potentially vulnerable to hardware failures and software bugs in addition to internal or external intrusions and these bugs can corrupt the health records. The malware programmes such as viruses, worms and Trojan horses can damage the computers by consuming memory after replicating itself, stealing passwords or files, spying on user activities or other computers on the same network and clogging networks. The unauthorized 'intruders' can break in to the EHR systems (hackers) by cracking password (crackers) or exploiting security weaknesses and can damage integrity and availability of the EHR systems by manipulating or destroying the data.

EHR related online activities may include electronic submission of claims, e-prescriptions and electronically exchanging patient information that will be dependent on cybersecurity practices to protect information and EHR systems necessitating strong cybersecurity practices in place. Cybersecurity detects and safeguards information or any digital resource in any digital memory device or computer by responding to attacks against a computer system and its information or to unauthorized access. Healthcare professionals frequently exchange patients' information through mobile phones, emails, and text messages among colleagues for consultation that are not entirely safe. Web-based access to health information has further complicated privacy issues. In

[174] Ibid.

his special editorial to CNN, Bruce Schneier[175] describes internet as a surveillance state and explains about internet security threats.

6.5. Unintended undesirable consequences

There are several unintended undesirable consequences related to EHR including increased medical errors, overdependence on technology, extended

[175] Bruce Schneier, 'The internet is a surveillance state' (16 March 2013). <http://edition.cnn.com/2013/03/16/opinion/schneier-internet-surveillance > accessed on 6 January 2017

"Whether we admit it to ourselves or not, and whether we like it or not, we're being tracked all the time. Google tracks us, both on its pages and on other pages it has access to. Facebook does the same; it even tracks non-Facebook users. Apple tracks us on our iPhone and iPads. One reporter used a tool called Collusion to track who was tracking him; 105 companies tracked his Internet use during one 36-hour period…… This ubiquitous surveillance. All of us being watched, all the time, and that data being stored forever. This is what a surveillance state looks like, and it's efficient beyond the wildest dreams of George Orwell."

He describes that computers are being used to do everything and data is created by computers as a natural by-product; all the data is being saved, combined and matched. Big-data companies build detailed profile of our lives by collecting data from different sources and make money out of it. Mr Schneier describes, how we are being monitored on daily basis through internet, email, cell phones, social networking sites, web browsing and search engines making almost impossible to maintain privacy on the internet.

"Maintaining privacy on the internet is nearly impossible. If you forget even once to enable your protections, or click on the wrong link, or type the wrong thing, and you've permanently attached your name to whatever anonymous service you're using. Monsegur slipped up once, and the FBI got him. If the director of the CIA can't maintain his privacy on the internet, we've got no hope."

In Schneier's view, governments and corporations are two powerful spying forces working together in a way that corporations collect data and the governments are happy to use this to spy on powerless (people); governments occasionally asking to collect more data and save it for longer period; corporations are content to buy data from governments, and he thinks, the governments and corporations are going to continue that way without giving up their positions despite peoples' demand. Mr Schneier continues to describe privacy status in the era of advanced technology:

"So, we're done. Welcome to a world where Google knows exactly what sort of porn you all like, and more about your interests than your spouse does. Welcome to a world where your cell phone company knows exactly where you are all the time. Welcome to the end of privacy conversations, because increasingly your conversations are conducted by e-mail, text, or social networking sites.

And welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent; and where the government accesses it at will without a warrant.

Welcome to an internet without privacy, and we've ended up here with hardly a flight.

EHR unavailability, speed of the system, changes in institutional power structure, negative emotions of end-users, and physicians' dissatisfaction.[176] Physicians find that computerized physician order entry (CPOE) has increased workload because of entering required information, responding to alerts, entering multiple passwords and, spending extra time.[177] Physicians sometimes inadvertently enter the wrong order by clicking on the adjacent patient's name or medication form.[178] Enforcing physicians through mandatory data entry fields alters the power structure of organization by reducing autonomy of physicians and enhancing powers of information technology staff, nurses and administration.[179] Intense emotions found among end-users usually cause reduced efficacy of use of the system.[180] Unexpected downtime can cause unavailability of basic medical care and disruption of routine clinical services. As it is becoming increasingly difficult for the organizations to work without it, alternative solutions and planning for management is required instead of overdependence on technology.[181] Other unintended and undesirable consequences described by Campbell and others, include unfavourable workflow issues, never-ending system demands, problems related to paper persistence and unfavourable changes in patterns and practices of communication.[182] The policymakers and individual organizations need to take steps to resolve these difficult ethical and legal challenges through appropriate laws and regulations.

6.6 Summary

The drawbacks of EHR including financial challenges, privacy and security issues have been explored. Brief description of fundamentals of ethics and ethical frameworks is provided to understand how the ethical principles of

[176] Emily Campbell, Dean Sitting, Joan Ash, and others, 'Types of Unintended Consequences Related to Computerized Provider Order Entry' (2006)13(5) J Am Med Inform Assoc 547.
[177] Joan Ash, Dean Sitting DF, Eric Poon, and others, 'The Extent and Importance of Unintended Consequences Related to Computerized Provider Order Entry' (2007)144(4) J Am Med Inform Assoc 415.
[178] Ibid.
[179] ibid.
[180] ibid.
[181] ibid.
[182] Campbell (n 176).

autonomy, beneficence, non-maleficence and justice apply to confidentiality issues of an integrated EHR system.

Chapter 7: Secondary uses of patient data – ethical and legal issues

The health information is collected to provide care for the patient. This information can be used for its original purpose called primary use, such as patient care delivery, patient care management, patient care support processes, patient self-management, financial and other administrative processes. Patient health information's use or reuse for different purposes, other than one for its acquisition, is a secondary use. GMC guidance 'Confidentiality' (2009) at paragraph 40 describes important secondary uses that include, 'research, epidemiology, public health surveillance, health service planning, and education and training.[183] There are motivations and challenges for secondary use of clinical data. In the preface to his book, 'Public Health Law', Lawrence O Gostin expressed his concern:

> Despite my background as a civil libertarian,…. I question the primacy of individual freedom (and the associated concepts of autonomy, privacy, and liberty) as the prevailing social norm. Freedom is a powerful and important idea, but I think scholars have given insufficient attention to equally strong values that are captured by the notions of partnership, citizenship, and community. As members of a society in which we all share a common bond, our responsibility is simply to defend our own right to be free from economic or personal restraint. We also have an obligation to protect and defend the community as a whole against threats to health, safety, and security. Each member of society owns a duty – one to another – to promote the common good. And each member benefits from participating in a well-regulated society that reduces risks that are common to all.[184]

The advantages and a few disadvantages of EHR have already been discussed in the previous chapter. Issues related to the use of confidential information for secondary purposes are discussed in this chapter.

[183] General Medical Council, 'Confidentiality' (2009). <http://www.gmc-uk.org/Confidentiality_0513_Revised.pdf_52090934.pdf> Accessed 12 January 2017.
[184] Lawrence O Gostin, *Public Health Law* (2nd edn, University of California Press 2008).

7.1. What is duty of confidence?

In the NHS Code of Practice (2003), at paragraph 9 it is stated that:

> A duty of confidence arises when one person discloses information to another (for example patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.[185]

In *Attorney-General v Guardian Newspapers (N0 2)*[186] Lord Goff stated (at p.658) that the:

> duty of confidence arises when confidential information comes to the knowledge of a person (the confident) in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others.

When someone is controlling his own personal information, that information is private; he has right to use or disclose that information, whereas confidentiality is the duty to protect the personal information that belongs to someone else, which was communicated in the circumstances (for example under medical care), with reasonable expectations to be kept confidential. Although the concepts of privacy and confidentiality are different but they are linked in a way that 'it's privacy, that drives the duty of confidentiality'[187].

In *Campbell v Mirror Group of Newspapers Ltd*.[188] Lord Nicholls commented on privacy and confidentiality:

> Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private.

[185] Department of Health, 'Confidentiality: NHS Code of Practice' (2003).
[186] [1990] AC 109.
[187] Peter Lennon, *Protecting Personal Health Information in Ireland: Law & Practice* (2005 Oak Tree Press) 67.
[188] [2004] UKHL 22 [15].

The position is clear that in the doctor-patient relationship, the duty of confidence exists between the patient and the doctor; as the nature of medical information and the circumstances in which it is communicated (the confident has notice or agrees that the information is confidential), fulfils its requirements.

7.2. Balancing competing interests for secondary uses of patient data

Decisions regarding disclosing confidential information for secondary use (for example research, public health, commissioning) involve balancing competing public interests against individual interests. The public wants evidence based safe and effective medical care whereas an individual (patient) does not want to be exposed to added health risks or damage his privacy. The question arises how to balance the competing interests of the society and the individual. The public interest in respecting individual's privacy and most individuals' interest in healthcare advancement through clinical research, are common interests. Therefore, it could be reasoned that the public's interest in maintaining confidence and public's interest in disclosing confidential information subject to justification of circumstances, could be potentially competing public interests.

Sharing of patient information among caring teams has become easier due to advanced technology and accessibility of the clinical information, whereas advanced technology has also increased pressure on policy makers, healthcare professionals and public to share patient information for research and other secondary purposes making it as important as to protect confidentiality. Caldicott's seventh principle, 'the duty to share information can be as important as the duty to protect patient confidentiality'[189] strengthens the need for sharing information.

[189] Department of Health, 'The Information Governance Review: To Share or Not to Share' [2013] <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf> accessed on 5 December 2016.

7.3. Interests in maintaining confidentiality

7.3.1. Duty of confidence and its sources

7.3.1.1. Ethical and professional basis

The Hippocratic Oath states: 'All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to spread abroad, I will keep secret and will never reveal.'[190]

The Declaration of Geneva states that: 'I will respect the secrets which are confided in me, even after the patient has died'.[191]

To justify the existence of a duty of confidence between doctors and patients, consequentialist and deontological reasoning can be used. The consequentialist reasoning can be, that the patients would be reluctant to seek treatment from their doctor if they did not believe that their confidentiality would be protected and the optimum medical care would not be possible. Deontological reasoning would be that the patient must be respected as autonomous agent (can make informed decisions, with available alternative options and lack of coercion), their right to privacy be respected and they should be able to control access to their personal and sensitive information. In neither case, the duty to maintain confidentiality is absolute.

The GMC guidance on confidentiality and supplementary guidance on specific situations do not have the force of law; however, the courts do consider them to have credible authority.

[190] Hippocratic oath, 'Mosby's Medical Dictionary' (10th edn Elsevier 2012).
[191] World Medical Association, 'Declaration of Geneva 2006' <www.wma.net/e/policy/c8.htm>

The GMC guidance, 'confidentiality (2009)', at paragraphs 6, 8 and 9 describes that in a doctor-patient relationship, confidentiality is vital because in its absence, the patient may be hesitant to provide necessary required information to the doctor for appropriate care due to loss of trust, but appropriate information sharing is also important for the delivery of safe and effective care to the individual patient and to the society.[192] The duty of confidence is not absolute and personal confidential information can be disclosed due to legal requirement or after appropriate patient consent or if it is justified in the public interest.[193] Paragraph 9, guides that for disclosure, anonymised or coded information must be used if practicable and satisfies the need, and the fully informed patient has no objection to disclosure; however, for identifiable information disclosure purposes, express consent should be obtained if disclosure is not for direct care or local clinical audit or if it is required by law or justified in public interest, and minimum necessary information should be disclosed after fulfilling relevant legal requirements including common law and the DPA 1998 requirements.[194]

This guidance makes it clear that the duty of confidence exists between healthcare professionals and the patients but it is not absolute and in certain circumstances disclosure can be made.

In GMC guidance document, 'General Medical Practice 2013', it states at paragraph 50 that: 'You must treat information about patients as confidential. This includes after a patient has died.'[195] However, DPA 1998 deals with living individuals, but GMC guidelines are clear that duty of confidence extends even a patient has died.

[192] GMC, 'Confidentiality' (2009) (n 183)
[193] Ibid 8
[194] ibid 9
[195] General Medical Council, 'Good Medical Practice' (2013), <http://www.gmc-uk.org/Good_medical_practice___English_1215.pdf_51527435.pdf> Accessed on 12 January 2017.

7.3.1.2. Legal sources

7.3.1.2.1. Common Law

In *Attorney-General v Guardian Newspaper (No 2)*,[196] Lord Bingham (at pp. 215-216) stated the duty of confidence comes from an obligation of conscience. 'It lies in the notion of an obligation of conscience arising from the circumstances in or through which the information was communicated or obtained.'

Lord Bingham explained that the duty of confidence originates from an obligation of 'conscience' in the 'circumstances' the information was 'communicated' or collected.

In *W v Egdell*,[197] W was a patient with mental problems who was detained in a secure hospital rather than a prison following convictions of killing five people and wounding two others. The defendant, consultant psychiatrist was instructed by the patient's solicitors to examine W and prepare a report with a view to use the report in supporting W's case at the tribunal for discharge or transfer to a regional unit. The solicitors withdrew the application after knowing that the report, had opposed the discharge or transfer based on conclusions that the patient was still a danger to the public. Dr Egdell sent a copy of the report to the hospital and to the Secretary of State, knowing that his opinion would not become part of the patient's clinical notes. W's solicitors sought an injunction and damages for breach of confidence. The Court of Appeal held that in the public interest, for protection of the public from dangerous criminal actions, the breach was justified. There is no doubt that a duty of confidence existed between Dr Egdell and the patient. Bingham LJ stated that:

[196] [1990] AC 109
[197] [1990] Ch 359

> It has never been doubted that the circumstances here were such to impose on Dr. Egdell a duty of confidence owed to W…It is not in issue here that a duty of confidence existed. The breadth of such a duty in any case is, however, dependent on circumstances.

7.3.1.2.2. Human Rights Act 1998 (HRA 1998)

Does Article 8 of the HRA 1998, the right to respect for private and family life protect a patient's interests in confidentiality? Article 8 provides

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

'Respect for private life' could include, keeping personal information (medical records) private and the confidentiality could be protected under Article 8(1). Article 8 right is not absolute, as 8(2) allows interference when necessary within appropriate situations, for example, 'for the protection of health or morals'.

In *Z v Finland* [198] case, where Z was married to someone who was HIV positive and was charged with several sexual offences. During investigation, police obtained his medical records. The European Court of Human Rights (ECtHR) accepted that the patient's rights to respect for the private and family life under Article 8 (1) had been interfered, therefore, considered whether requirements of Article 8 (2) were satisfied and held that the measures taken were not disproportionate as a 'legitimate aim' was being pursued. The judgment of the ECtHR states:

[198] [1998] 25 EHRR 371.

> The court accepts that the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings, where such interests are shown to be of even greater importance.

In *Campbell v Mirror Group Newspapers Ltd*,[199] where, it was to determine whether the press's freedom to publish the model Naomi Campbell's drug addiction treatment information should take priority over her right to privacy. The House of Lords found that because of the nature of the information about the model Ms Campbell's drug addiction treatment, an obligation of confidence existed. Then, Article 10 of the HRA 1998 was considered, but it was held that Ms Campbell's right to privacy outweighed MGN's right to freedom of expression.

The case highlights that when under common law duty of confidence, the ways to protect or disclose the confidential information should respect a patient's reasonable expectations of privacy.[200]

7.3.1.2.3. Data Protection Act 1998

The definitions relevant to the DPA 1998, Data Protection Principles, Schedule 2 and relevant part of Schedule 3 are provided in chapter 2. The first and second data protection principles are discussed below to address the issues raised in this chapter.

Data Protection Principle One:

> Personal data shall be processed fairly and lawfully and, shall not be processed unless-
>
> (a). at least one of the conditions in Schedule 2 is met, and
>
> (b). in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

[199] [2004] 2 All ER 995.
[200] Ibid [22]

'Fair processing information' sets out data controller's obligations under Schedule 1, Part 2 of DPA 1998, that information to be supplied to the 'data subject': the identity of the data controller (para 2(3)(a)), and the purpose or purposes for which the data are intended to be processed (para 2(3)(c)).

The 'fair information processing' obligation does not apply to the section 29 (regarding detection and prevention of crime), section 31 (regarding protection of public members against 'dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity' (section 31(2)(a)(iii)), and section 35 (regarding 'disclosures required by law or made in connection with legal proceedings etc').

In processing data 'lawfully', the common law requirements of confidentiality and European Convention on Human Rights requirements become relevant. This means that without satisfying the relevant confidentiality requirements of common law, the processing of personal data will not be lawful.

The other requirement of the first principle of the DPA 1998 is, that at least one condition of Schedule 2, and in case of sensitive personal data, at least one condition of Schedule 3 must be satisfied.

Data Protection Principle Two:

> Personal data should be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

There is an exception to the second Data Protection Principle 2, in section 33 where the processing is for the research purposes.

7.3.1.2.4. Remedies

Three different remedies are available under DPA 1998, if there is breach of these provisions. The data subject can write to data controller under section 10 of DPA 1998 to request to stop from processing his personal data and needs to establish the grounds such as that processing is causing or is likely to cause substantial damage to him or third party (section 10(1)). If the data subject or another has suffered damage or consequent damage due to disclosure, he can seek compensation under section 13 of DPA 1998. However, the data controller will have a defence if he can show that the reasonable care was taken to comply with the requirement of the Act. The court can order the data controller under section 14 of DPA 1998, to block, rectify, erase or destroy inaccurate data.

7.4. Circumstances permitting disclosure of confidential information

There are three broad exceptions to the duty of confidentiality where identifiable health information can be disclosed. These exceptions include:

- Where disclosure is required by the law.
- Where appropriate consent is present.
- Where public interest is overriding.

7.4.1. Disclosures required by law

There are circumstances where healthcare professionals have statutory obligations to disclose patient confidential information such as serious communicable diseases (Public Health (Control of Disease) Act 1984, Public Health (Infectious Diseases) Regulations 1998) and in the interest of order and justice (Police and Criminal Evidence Act 1984); the patients' consent to disclosure is not necessary. Other Acts and Regulations include Abortion Regulations 1991, Births and deaths Regulations Act 1953, Road Traffic Act 1988, Human Fertilisation and Embryology Act 1990, NHS (Venereal Diseases) Regulations 1974, Children Act 1989, Prevention of Terrorism (Temporary Provisions) Act 2000. Patients generally should be informed that the disclosure is to a secure authority, but they have no right to refuse. The NHS Code of Practice (2003) at paragraph 50 states that the courts have

legal powers to obtain the confidential information relevant to the matters in the court."[201]

7.4.2. Disclosure with consent

Mental Health Act 1983 Code of Practice (revised 2008) provides definition of consent:

> Consent is the voluntary and continuing permission of a patient to be given a particular treatment, based on a sufficient knowledge of the purpose, nature, likely effects and risks of that treatment, including the likelihood of its success and any alternatives to it. Permission given under any unfair or undue pressure is not consent.[202]

For consent to be valid

i. The patient must have capacity,
ii. Consent must be given voluntarily (with no deceit or coercion)
iii. Must be provided adequate information about the treatment to which the patient is being consented to reach a decision.

The consent may be explicit or implied but in both situations, it needs to be informed consent. It can be oral, written or partly oral and partly written. For healthcare professionals, it is always safer to get explicit or express written consent especially for invasive procedures.

7.4.2.1. Explicit or Express consent

Explicit or express consent is obtained when a patient actively agrees orally or in writing to that specific use, or disclosure of confidential information, or explicitly consents to future uses that have been explained to the patient.

GMC guidance, Confidentiality (2009), emphasis at paragraph 33 that before disclosing identifiable information for secondary purposes (other than direct

[201] 'Confidentiality: NHS Code of Practice' (2003) (n 185) para 50
[202] Mental Health Act 1983 Code of Practice (revised 2008).

care, local clinical audit and so on) express consent should be obtained.[203] At paragraph 41 it states further that 'for many secondary uses' disclosing anonymised or coded data 'will be sufficient and practicable', however, express consent would be appropriate if disclosure requires identifiable information or removal of identifiers is not practicable.[204]

7.4.2.2. Implied Consent:

The action by the behaviour of an informed competent patient may imply that the patient has given consent. GMC guidance, 'Consent: patients and doctors making decisions together' (2008), states at paragraph 45:'Patients can give consent orally or in writing, or they may imply consent by complying with the proposed examination or treatment, for example, by rolling up their sleeve to have their blood pressure taken.'[205]

The GMC guidance, Confidentiality (2009) at paragraph 25 indicates that based on implied consent, information can be shared among 'healthcare team' 'and other staff who support the provision of their care' [206]

7.4.3. Disclosure in the public interest

7.4.3.1. Common Law

Paula Case describes position of common law in confidentiality as:

> The common law's position on this issue is far clear, but neither implied consent nor the public interest defence appear to be sufficiently robust to afford protection to medics who disclose patient information for the purposes of medical research or general public health surveillance. As decision-makers in the balancing of public interest factors, such as the protection of informational autonomy *vs.* the advancement of medical

[203] GMC, 'Confidentiality' (2009) (n 183) para 33
[204] ibid 41
[205] General Medical Council, 'Consent: Patients and Doctors Making Decisions Together' (2008), <http://www.gmc-uk.org/GMC_Consent_0513_Revised.pdf_52115235.pdf> Accessed on 12 January 2017.
[206] GMC, 'Confidentiality' (2009) (n 183) para 25.

> intelligence, we could do much worse than the courts who have demonstrated a departure from the 'light touch' regulatory approach associated with the *Bolam* test. The greatest defect of the common law has, however, been beyond the courts' power to correct.[207]

In *Attorney General v Guardian Newspapers (No 2)*[208] Lord Griffith commented: 'This involves the judge in balancing the public interest in upholding the right to confidence … against some other public interest that will be served by the publication of the confidential material.'

And Lord Goff stated: '…although the basis of the law's protection of confidence is that there is a public interest that confidences should be preserved and protected by the law, nevertheless that public interest which favours disclosure.'

The case emphasis **balancing and proportionality approach** in circumstances where interests in maintaining confidence are competing against disclosing confidential information.

In *X v Y*,[209] health authority employees provided a newspaper identity of two practicing doctors with AIDS. The newspaper already had published general article concerning doctors with AIDS practicing in Britain and wanted to publish further article with information that identified the doctors. The health authority sought an injunction to prevent the defendants from publishing the identity of the two doctors and was granted. The Court balanced the public interest in maintain hospital records confidence against the public interest in freedom of the press; and found that lack of publication would be of minimal significance. Rose J stated that it would be in the interest of public that confidence be maintained.

[207] Paula Case, 'Confidence Matters: The Rise and Fall of Informational Autonomy in Medical Law' (2003) 11 Med L Rev 208.
[208] [1990] AC 109.
[209] [1988] 2 All ER 648

The application of competing public interests was also demonstrated in *H (A Healthcare Worker) v Associated Newspapers Ltd*,[210] in which the Court of Appeal found strong public interest in maintaining the confidentiality of HIV infected health workers.

In *W x Egdell*,[211] the Court of Appeal held that the disclosure is justified in the public interests when balancing confidentiality against safety of the public from dangerous criminal acts that the patient had committed and the necessity to inform the relevant authorities about his medical condition so that they will be in a better position to make decisions about his release.

7.4.3.2. Professional guidance

The GMC guidance 'Confidentiality' (2009) attempts to reconcile the confidence interest and the disclosure interest issues in paragraphs 36-39.

> Confidential medical care is recognised in law as being in the public interest. However, there can also be a public interest in disclosing information: to protect individuals or society from risks of serious harm, such as serious communicable diseases or serious crime; or to enable medical research, education or other secondary uses of information that will benefit society over time.[212]

The paragraph 37 confirms that the personal information can be disclosed in public interest without patient's consent in special circumstances.[213] The paragraph 38 emphasises that the need for identifiable information should be satisfied if anonymisation is not practicable.[214]

[210] [2002] EWCA Civ 195.
[211] [1990] Ch 359
[212] GMC, 'Confidentiality' (2009) (n 183) para 36.
[213] ibid 37
[214] ibid 38

The guidance at paragraph 51, stresses on encouraging patients to disclosures that are considered necessary for their protection and informing about risks of refusing to consent but competent adult patient's refusal should be respected.[215] Paragraph 53 of the guidance becomes relevant if others are exposed to a risk of death or serious harm due to failure to disclosure; in these circumstances disclosure of personal information 'without consent may be justified'.[216] Paragraph 55 guides to disclose information 'promptly to an appropriate person or authority' in the circumstances 'when the others are exposed to a risk so serious that it outweighs the patient's and the public interest in maintaining confidentiality', if the patient refuse to consent, 'or if it is not practicable or safe' to obtain the patient's consent.[217]

NHS Code of Practice at paragraphs 31, 33 and 34, provides guidance regarding disclosure in circumstance where it's difficult for staff to make decision. At paragraph 31 the Code advises that a clear record of the decision making process and the advice sought, must be made 'in the interest of both staff and organisation they work within' when 'disclosure to the courts and to regulatory bodies' is justified.[218] At paragraph 33, the Code guides that in difficult and finely balanced decisions, it may be necessary to obtain advice from legal or from 'professional, regulatory or indemnifying bodies' 'or to await or seek a court order'.[219]

At paragraph 34, the Code states that if there is significant public interest in disclosure, proportionality is the key principle and it further clarifies that if consent can be obtained then disclosing confidential information to a researcher would be unreasonable and disproportionate, however, if obtaining consent is not practicable and locating patient is difficult with reasonable

[215] ibid 51
[216] ibid 53
[217] ibid 55
[218] Confidentiality, NHS Code of Practice (2003) (n 185) para 31
[219] ibid 33

efforts and the risk to the patient is negligible, disclosing information for research is proportionate.[220]

7.5. Section 251 and Section 252 of National Health Service Act 2006

Section 251 of the National Health Service Act 2006 gives powers to the Secretary of State for Health to make regulations to allow use of confidential patient information without patient consent in special circumstances. The use of this power is allowed for medical purposes, for the patient or the public interest, where consent is not practicable and anonymised information will not satisfy the cause. After recognising that some necessary NHS functions and significant medical research require patients' identifiable information use and in the absence of, appropriate disclosure consent and secure legal basis, section 251 and accompanying regulations were enacted. Confidentiality advisory group (CAG) advises on section 251 after considerations to public interest (balancing public good and risk to individual from disclosure), data protection (fair processing, minimal information satisfying the purpose requirement and management of data after end of research) and reasons of not obtaining patient consent or using pseudonymised data. It also provides definitions of 'patient information', 'confidential patient information' and 'medical purposes'.

7.6. Anonymisation and Pseudonymisation of data

Anonymised data is defined as the 'data relating to a specific individual where the identifiers have been removed to prevent identification of that individual'.[221] In the glossary of terms, the GMC 'Confidentiality (2009) provides meaning of the term 'anonymised information':

> Information from which individuals cannot reasonably be identified. Names, addresses, full postcodes or identification number, alone or together or in conjunction with any other information held by or available to the recipient, can be used to identify patients.[222]

[220] ibid 34
[221] *Open Data White Paper* (n 13).
[222] Confidentiality, NHS Code of Practice (2003) (n 185)

Pseudonymised data is defined as the 'data relating to a specific individual where the identifiers have been replaced by artificial identifiers to prevent identification of the individual'.[223]

For practical purposes the anonymised data is not confidential data and regulations will not be made under section 251 of the National Health Service Act 2006.

In *R v Department of Health, ex parte Source Informatics Ltd*,[224] the issue of the use of anonymised patient data acquired from prescription forms, was considered. The GP prescription forms contained the name and quantity of the product, which had commercial value to the pharmaceutical companies. The Department of Health issued advice stating that GPs and pharmacists should abstain from the scheme because anonymisation of information did not remove the duty of confidence owed to patients. The applicants sought a declaration from the court against the policy of the Department of Health. Latham J, held that in the absence of patient consent, disclosure of anonymised information could constitute the breach of confidence and the application of Source Informatics Ltd was rejected. The Court of Appeal allowed the appeal. Simon Brown LJ concluded that the case did not involve breach of confidence as the patients' identities are anonymised and protected: 'The patient's privacy will have been safeguarded, not invaded. The pharmacist's duty of confidence will not have been breached.'

The Court of Appeal decision established that disclosure of anonymised information is not a breach of confidence.

The re-identification of patients from anonymised data, especially those with rare conditions, has been demonstrated[225]. Undoubtedly 'anonymous' data (is a data that never had any identifiers) falls outside the scope of Directive

[223] *Open Data White Paper* (n 13).
[224] [2001] QB 424
[225] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701.

95/46/EC, but in case of 'anonymised' data where identifiers have been removed (through 'processing'), application of the Directive is arguable. the DPA 1998 will apply to processing of that data once the identifiable data is linked with the individual. The common law position is that anonymised data is not confidential but the anonymisation requires processing of identifiable data and DPA 1998 applies to the processing of identifiable data. Emily Jackson commenting on *R v Department of Health ex parte Source Informatics*, in her book 'Medical Law', and several other critics have raised several questions regarding the Court decision.[226,227] The questioned whether anonymising data removes its confidential nature, is still unclear ? There is a difference between anonymous data and anonymised data. Anonymised data is a processed data where identifiers have been removed whereas anonymous data never had any identifiers.

7.7. Summary

The legal framework and professional guidance has shown that the legal duty of confidentiality is not absolute and identifiable data can be used for secondary purposes without consent, if such use is necessary and is **proportionate** with respect to privacy and **public interests**. Whenever possible, personal health data used for secondary purposes should be anonymised and if it is not practicable or if there is need for use of identifiable data, express consent should be used, however, some disclosures without consent may be legitimate in relation to NHS financial management needs; for research purposes if it is in public interest. The critics have argued that the notion of anonymised data not being confidential is challengeable and in future its legal position might change. More research and consultation on anonymisation issue, opt-out grounds, justifications, designs and consent forms is needed.

[226] Emily Jackson, '*Medical Law: Text, Cases, and Materials*'. (2nd edn, OUP 2010) 382.
[227] Jose Miola, 'Owing Information – anonymity, confidentiality and human rights' (2008) 3 Clinical Ethics 116.

Chapter 8: Conclusion

The purpose of this thesis was to provide an understanding of EHR, its uses, advantages, disadvantages, ethical and legal aspects focusing on the issues arising from sharing of health records for secondary purposes. The need for this thesis has arisen due to public concerns about the adequacy of current controls and safeguards, and opportunities related to the use of patient confidential information for purposes other than direct patient care.

The disclosure of confidential patient information without explicit consent, selling of anonymised patient data and reports of security breach have weakened patients' trust in the system. Privacy, security, confidentiality and consent are important ethical and legal concepts surrounding the current debate of patients' health records and its secondary uses. While this debate continues as to whether the existing privacy and security measures are adequate or not, secondary use of health records without consent is ethically justified or not, opt-out option makes patients' privacy protected or its ramifications further complicate the existing issues; it certainly has increased public awareness of privacy, confidentiality and security of health information.

Healthcare providers and policy makers are under pressure to utilise the maximum benefits of advanced technology. Patients expect high quality, safe and effective healthcare system, which can restore their trust and ensure that their health information will remain confidential and secure. Healthcare professionals need user-friendly information systems to have prompt, easy, uninterrupted and secure access to the complete, accurate, valid and up to date health records, to make informed choices and evidence based decisions for provision of 'demanded' high quality, safe and effective service to the patients. To some extent EHR systems have met these demands and have

provided exciting opportunities of enabling data for secondary uses, but it has also contributed to concerns over privacy, confidentiality and data protection. Lack of clarity and transparency in the management of patients' health data, and loss of traditional control over personal health data is being perceived as loss of autonomy.

Three independent reviews commissioned by the secretary of state have been published in 2016, highlighting public concerns related to secondary use of health data, security and confidentiality along with some recommendations. Lack of public awareness about health data, its secondary uses and benefits to both individual patients and the society; absence of transparency in management of health data; unclear terminology such as anonymisation; insufficient public consultation; impulsive and poorly planned policies with inappropriate leadership; disproportionate and insufficiently trained implementing and monitory staff with inadequate immediate support and funding; dispossession of responsibility and top-down policy; and above all disinterest in finding remedies for diminishing altruism in the society are the major issues destroying public trust that need to be addressed on urgent basis.

Public trust in health data can be restored by transparent activity in the management of health data, better information sharing and making shared decisions. Achieving balance between public interest in respecting confidentiality and public interest in sharing health data for secondary purposes will require open national debate and wide consultation, engaging public in medical research by providing information to develop understanding of research, bottom up policy, improved practices and patience to allow these changes. Meanwhile, there are some interim solutions such as improved consent forms that can satisfy patients' concerns, dissemination of information leaflets in simple and easy to understand language, as well as utilization of modern internet technology for public awareness.

The thesis concludes on a comment from Robert Wachter's review, 'Making IT Work': 'It would be a mistake to lock down everyone's healthcare data in the name of privacy'…and…'the one thing that NHS cannot afford to do is to remain a largely non-digital system'.[228]

[228] National Advisory Group on Health Information Technology in England, 'Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England' London: Department of Health, August 2016. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550866/Wachter_Review_Accessible.pdf > Accessed on 18 January 2017.

Table of Cases

Attorney General v Guardian Newspapers (No 2) [1990] AC 109

Campbell v Mirror Group Newspapers Ltd [2004] 2 All ER 995

H (A Healthcare Worker) v Associated Newspapers Ltd [2002] EWCA Civ 195.

R v Department of Health, ex parte Source Informatics Ltd [2001] QB 424

W x Egdell [1990] Ch 359

X v Y [1988] 2 All ER 648

Z v Finland [1998] 25 EHRR 371

Table of Legislation

Access to Health Records Act 1990

Access to Medical Records Act 1988

Data Protection Act 1998

Electronic Communication Act 2000

Environmental Information Regulations 2004

Freedom of Information Act 2000

Health and Social Care Act 2008

Health and Social Care Act 2012

Human Rights Act 1998

Mental Capacity Act 2005

NHS (Venereal Diseases) 1974 Regulations

Re-use of Public Sector Information Regulations 2005

National Health Service Act 2006

The Access to Medical Reports Act 1988

The Computer Misuse Act 1990

The Terrorism Act 2000

Bibliography

Books:

1. Bauchamp T and Childress J, *Principles of Biomedical Ethics* (1st edn OUP 1979)
2. Bemmel Jand and Musen M, *Handbook of Medical Informatics* (Springer 1997)
3. Benson T, *Principles of Health Interoperability HL7 and SNOMED* (Springer 2009)
4. Duquenoy P, George C and Kimmpa K, '*Ethical, Legal and Social Issues in Medical Informatics'* (2008) IGI Global
5. George C and Whitehouse D and Duquenoy P, *eHealth: Legal, Ethical and Governance Challenges* (Springer 2012).
6. Gostin L, *Public Health Law* (2nd edn, University of California Press 2008)
7. Hoyt R and Yoshihashi A, *Health Informatics: Practical Guide for Healthcare and Information Technology Professionals* (6th edn, Lulu.com, Pensacola, Fl)
8. Jackson E, *Medical law: text, cases, and materials* (2nd edn, OUP 2010).
9. Jonsen A and Siegler M and Winslade W, *Clinical ethics* (6th edn, McGraw-Hill 2006).
10. Lennon P, *Protecting Personal Health Information in Ireland: Law & Practice* (Oak Tree Press 2005)
11. Schaller B, *Understanding Bioethics and the Law: The Promises and Perils of the Brave New World of Biotechnology* (Praeger 2008)
12. Shortliffe E and Cimino J, *Biomedical Informatics* (3rd edn, Springer 2006)

Official Documents

1. CQC, *Safe data, safe care* (2016) <http://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf> accessed on 5 Dec 2016.
2. Department of Health, *Confidentiality: NHS Code of Practice* (2003).
3. Department of Health, *Guide to the Healthcare System in England (2013)* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/194002/9421-2900878-TSO-NHS_Guide_to_Healthcare_WEB.PDF
4. Department of Health, *Guide to the Healthcare System in England*' (2013). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/194002/9421-2900878-TSO-NHS_Guide_to_Healthcare_WEB.PDF
5. Department of Health, National Advisory Group on Health Information Technology in England, *Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England*' (2016). <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550866/Wachter_Review_Accessible.pdf > Accessed on 18 January 2017.
6. Department of Health, National Advisory Group on Health Information Technology in England, *Making IT Work: Harnessing the Power of Health Information Technology to Improve Care in England* (2016). <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550866/Wachter_Review_Accessible.pdf > accessed on 18 January 2017.
7. Department of Health, *Personalised Health and Care 2020*. (2014)
8. Department of Health, *Protection and Use of Patient Information: Guidance on confidentiality*. (1996).
9. Department of Health, *Structure of Public Health England (2012)* <http://www.rcpsych.ac.uk/pdf/Structure%20of%20Public%20Health%20England.pdf> accessed on 6 January 2017.

10. Department of Health, *The Information Governance Review: To Share or Not to Share*'(2013) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf> accessed on 5 December 2016.
11. Department of Health. *Review of Data Security, Consent and Opt-Outs* <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF> accessed on 4 December 2016).
12. General Medical Council, 'Confidentiality' (2009). <http://www.gmc-uk.org/Confidentiality_0513_Revised.pdf_52090934.pdf> accessed 12 January 2017.
13. General Medical Council, *Consent: Patients and Doctors Making Decisions Together* (2008), <http://www.gmc-uk.org/GMC_Consent_0513_Revised.pdf_52115235.pdf> Accessed on 12 January 2017.
14. General Medical Council, *Good Medical Practice* (2013) <http://www.gmc-uk.org/Good_medical_practice___English_1215.pdf_51527435.pdf> Accessed on 12 January 2017.
15. House of Parliament, *Electronic Health Records* (2015) Postnote 519
16. HSCIC, Academy of Medical Royal Colleges, *Standards for the clinical structure and content of patient records* (2013). <https://www.rcplondon.ac.uk/projects/outputs/standards-clinical-structure-and-content-patient-records> accessed on 10 January 2017.
17. NHS England, *Five Year Forward View* (2014).
18. NHS England, Understanding the New NHS (2014) < https://www.england.nhs.uk/wp-content/uploads/2014/06/simple-nhs-guide.pdf> accessed on 6 January 2017.
19. The Minister for the Cabinet Office, *Open Data White Paper* (CM 8353, June 2012. <https://data.gov.uk/sites/default/files/Open_data_White_Paper.pdf> accessed on 11 January 2017.

20. Thomas Powel, *The structure of the NHS in England* (House of Commons Library Briefing Paper CBP 07206, 2016) <http://www.nhshistory.net/Parliament%20NHS%20Structure.pdf>

International Treaties and International Official Papers

1. Government of Canada Panel on Research Ethics, 'Privacy and Confidentiality'. <http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/chapter5-chapitre5/ > accessed on 7 January 2017.
2. HIPAA, 'Summary of the HIPAA Security Rule' <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> (accessed on 2 January 2017).
3. ISO standard, ISO 15489-1:2016. Information and documentation – Records management. <http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542> accessed on 10 January 2017.
4. ISO TR 20514:2004 Health Informatics – 'EHR Definition, Scope, & Context.' <http://tc215.behdasht.gov.ir/uploads/244_514_ISO_TR_20514_2005(E)> accessed on 24 November 2016.
5. US Department of Health and Human Services Office for Civil Rights, 'Breaches affecting 500 or individuals' <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf> (Accessed on 3 January 2017).
6. World Medical Association, 'Declaration of Geneva 2006' www.wma.net/e/policy/c8.htm

Journal Articles

1. Agrawal A, 'Return on Investment Analysis for a Computer-Based Patient Record in the Outpatient Clinic Setting' (2002) 13(3) J Assoc Acad Minor Phys 61

2. Anderson R, 'Information Technology in Medical Practice: Safety and Privacy Lessons from the United Kingdom' (1999) (14) Medical Journal of Australia 181, 170
3. Anderson R, 'NHS-Wide Networking and Patient Confidentiality' (1995) 5 BMJ 31
4. Ash J, Sitting D, Poon E, Guappone K, Campbell E, Dykstra R, 'The Extent and Importance of Unintended Consequences Related to Computerized Provider Order Entry' (2007)144(4) J Am Med Inform Assoc 415
5. Balas A, Jaffrey F, Kuperman G, Boren S, Brown G, Pinciroli F, Mitchel J, 'Electronic Communication with Patients. Evaluation of Distance Medicine Technology' (1997) 278(2) JAMA 152
6. Barnett O, 'The application of computer-based medical-record systems in ambulatory practice' (1984) 310 NEJM 1643
7. Bates D, Gawande A, 'Improving Safety with Information Technology' (2003) 348(25) NEJM 2526.
8. Bates D, Leape L, Cullen D, Laird N, Petersen L, Teich J, Burdick E, Hickey M, Kleefield S, Shea B, Vliet M, Seger D, 'Effect of Computerized Physician Order Entry and a Team Intervention on Prevention of Serious Medication Errors' (1998)280(15) JAMA 1311
9. Bates D, Teich J, Lee J, Seger S, Kuperman G, Ma'Luf N, Boyle D, Leape L, 'The Impact of Computerized Physician Order Entry on Medication Error Prevention' (1999)6(4) J Am Med Inform Assoc 313
10. Benitez K, Malin B, 'Evaluating Re-Identification Risks with Respect to The HIPAA Privacy Rule' (2010) 17(2) JAMIA 169
11. Bhattacherjee A, Hikmet N, Menachemi N, Kayhan V, Brooks R, 'The Differential Performance Effects of Healthcare Information Technology Adoption' (2007) 24(1) Information Systems Management 5
12. Blumenthal D, 'Wiring the Health System – Origins and Provisions of a New Federal Program' (2011) 365(24) NEJM 2323
13. Blumenthal D, Glaser J, 'Information Technology Comes to Medicine' (2007)356(24) NEJM 2527

14. Campbell E, Sitting D, Ash J, Guappone K, Dykstra R, 'Types of Unintended Consequences Related to Computerized Provider Order Entry' (2006)13(5) J Am Med Inform Assoc 547
15. Case P, 'Confidence Matters. The Rise and Fall of Informational Autonomy in Medical Law' (2003) 11 Med L Rev 208
16. Chen P, Tanasijevic M, Schoenenberger R, Fiskio J, Kuperman G, Bates D, 'A Computer-Based Intervention for Improving the Appropriateness of Antiepileptic Drug Level Monitoring' (2003) Am J Clin Pathol 432
17. Cresswell K, Sheikh A, 'The HNS Care Record Service (NHS CRS): Recommendations from the Literature on Successful Implementation and Adoption' (2009) 17(3) Informatics in Primary Care 153
18. Day M, 'Patients can Opt out of Controversial National Records System' (2007)334(7583) BMJ 12
19. Devine E, Hansen R, Wilson-Norton J, Lawless M, Fisk A, Blough D, Martin D, Sullivan S, 'The impact of computerized provider order entry on medication errors in a multispecialty group practice' (2010)17(1) J Am Med Inform Assoc 78
20. Dexter P, Perkins S, Overhage M, Maharry K, Kohler R, McDonald C, 'A Computerized Reminder System to Increase the Use of Preventive Care for Hospitalized Patient' (2001) 345(3) NEJM 965
21. Erstad T, 'Analyzing Computer Based Patient Records: A Review of Literature' (2003) 17(4) J Healthc Inf Manag 51
22. Everett J, 'A Decision Support Simulation Model for the Management of an Elective Surgery Waiting System' (2002) 5(2): Health Care Manag Sci 89
23. Ewing T, Cusick D, 'Knowing what to Measure' (2004) 58(6) Healthcare Financial Management 60
24. Fleming N, Culler S, McCorkle R, Becker E, Ballard D, 'The Financial and Nonfinancial Costs of Implementing Electronic Health Records In Primary Care Practices' (2011) 30(3) Health Aff (Millwood) 481

25. Garde S, Knaup P, Hovenga E, Heard S, 'Towards Semantic Interoperability for Electronic Health Records' (2007) 46(3) Methods of Information in Medicine 332
26. Gelzer R, Hall T, Liette E, Reeves M, Sundby J, Tegen A, Warner D, Wiedemann A, McCormick K, 'Auditing Copy and Paste' (2009) 80(1) J AHIMA 26
27. Grace J, Taylor M, 'Disclosure of Confidential Patient Information and the Duty to Consult: The Role of the Health and Social Care Information Centre' (2013) 21 Medical law Review 415
28. Gunter T, Terry N, 'The Emergence of National Electronic Health Record Architectures in the United States and Australia Models, Costs and Questions' (2005) 7(1) Journal of Medical Internet Research e3
29. Hall M, Schulman K, 'Ownership of Medical Information' (2009) 301(12) JAMA 1282
30. Harman L, Flite C, Band K, 'Electronic Health Records: Privacy, Confidentiality and Security' (2012) 14(9) VM 712
31. Hirschtick R, 'A Piece of My Mind. Copy and paste' (2006) JAMA 295
32. Hunt D, Haynes B, Hanna S, Smith K, 'Effects of Computer-Based Clinical Decision Support Systems on Physician Performance and Patient Outcomes: A Systematic Review' (1998) 280(15) JAMA 1339
33. Johnston M, Langton K, Haynes B, Mathieu A, 'Effects of Computer-Based Clinical Support Systems on Clinician Performance and Patient Outcome. A Clinical Appraisal of Research' (1994) 120(2) Am Intern Med 135
34. Krishna S, Andrew Balas E, Spencer D, Griffin J, Boren S, 'Clincal Trials of Interactive Computerised Patient Education: Implications for Family Practice' [1997] 45(1) J Fam Prac 25
35. Kucher N, Koo S, Quiroz R, Cooper J, Paterno M, Soukonnikov B, Goldhaber S, 'Electronic Alerts to Prevent Venous Thromboembolism Among Hospitalized Patients' (2005) 352(10) NEJM 969
36. Kuperman G, Gibson R, 'Computer Physician Order Entry: Benefits, Costs, and Issues' (2003) 139(1) Annals of International Medicine 31

37. Ledwich L, Harrington T, Ayoub W, Sartorius J, Newman E, 'Improved Influenza and Pneumococcal Vaccination in Rheumatology Patients Taking Immunosuppressants Using an Electronic Health Record Best Practice Alert' (2009) 61(11) Arthritis Rheum 1505
38. Liebow E, Derzon J, Fontanesi J, Favorretto A, Baetz R, Shaw C, Thopson P, Mass D, Christenson R, Epner P, Snyder S, 'Effectiveness of Automated Notification and Customer Service Call Centres for Timely and Accurate Reporting of Critical Values: A Laboratory Medicine Best Practices Systematic Review and Meta-Analysis' (2012) 45(0) Clinical biochemistry 979
39. Liederman E, Morefield C, 'Web Messaging: A New Tool for Patient-Physician Communication' (2003) 10(3) J Am Med Inform Assoc 260
40. Lohr K, 'Outcome Measurements: Concepts and Questions' (1988) 25(1) Inquiry 37
41. Lohr K, Schroeder S, 'A Strategy for Quality Assurance in Medicine' (1990) 322 NEJM 1161
42. Mandl K, Szolovits P, Kohane I, 'Public Standards and Patients Control: How to Keep Electronic Medical Records Accessible but Private' (2001)322(7281) BMJ 283
43. Mangalmurti S, Murtagh L, Mello M, 'Medical Malpractice Liability in the Age of Electronic Health Records' (2010) (21) NEJM 2060, 363
44. McDonald C, 'Protocol-Based Computer Reminders, The Quality of Care, and the Non-Perfectibility of Man' (1976) 295 NEJM 1351
45. McDonald C, Hui S, Smith D, Tierney W, Cohen S, Weinberger M, McCabe G, 'Reminders to Physicians from an Introspective Computer Medical Record: A Two-Year Randomised Trial' (1984) 100 Annals of Internal Medicine 130
46. McDonald C, Hui S, Tierney W, 'Effects of Computer Reminders for Influenza Vaccination on Morbidity During Influenza Epidemics' (1992)9(5) MD Comput 304
47. McGraw D, 'Building Public Trust in Uses of Health Insurance Portability and Accountability Act De-Identified Data' (2013) 20(1) JAMIA 29

48. Menachemi N, Collum T, 'Benefits and Drawbacks of Electronic Health Record Systems' (2011) 4:47 Risk Management and Healthcare Policy 55
49. Mildon J, Cohen T, 'Drivers in the Electronic Medical Records Market' (2001) 22 Health Manag Technol 14
50. Miola J, 'Owing Information – anonymity, confidentiality and human rights' (2008) 3 Clinical Ethics 116.
51. Overhage M, Suico J and McDonald C, 'Electronic Laboratory Reporting: Barriers, Solutions and Findings' (2001) 7(6) J Public Health Manag Pract 60
52. Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701
53. Peterson L, Brennan T, O'Neil A, Cook F, Thomas Lee, 'Does House Staff Discontinuity of Care Increase the Risk for Preventable Adverse Events?' (1994) 121(11) Ann Intern Med 866
54. Rodwin M, 'The Case for Public Ownership of Patient Data' (2009) 302(1) JAMA 86
55. Rothstein M, 'The Role of Law in the Development of American Bioethics' (2009) 20(4) J Int Bioethique 73
56. Schiff G, Klass D, Peterson J, Shah G, Bates D, 'Linking Laboratory and Pharmacy: Opportunities for Reducing Errors and Improving Care' (1993)163 (8) Arch Intern Med 893
57. Schmidt I, Svarstad B, 'Nurse-Physician Communication and Quality of Drug Use in Swedish Nursing Homes' (2002) 54(12) Soc Sci Med 1767
58. Schneider G, Snell L 'CARE: An Approach for Teaching Ethics in Medicine' (2000) 51 Social Science and Medicine 1563
59. Shea S, Starren J, Weinstock R, Knudson P, Teresi J, Holmes D, Palmas W, Field L, Goland R, Catherine Tuck, Hripcsak G, Capps L, Liss D, 'Columbia University's Informatics for Diabetes Education and Telemedicine (Ideatel) Project: Rationale and Design' (2002) 9(1) J Am Med Inform Assoc 49
60. Sitting D, Stead W, 'Computer-based physician order entry: The state-of-the-art' (1994) 1 J Am Med Inform Assoc 108

61. Smith S and Denley I, 'Privacy in Clinical Information Systems in Secondary Care' [1999] BMJ 1328
62. Sterckx S, Rakic V, Cockbain J and Borry P, 'You Hoped We Would Sleep Walk into Accepting the Collection of Our Data: Controversies Surrounding the UK Care.Data Scheme and Their Wider Relevance for Biomedical Research' (2016) 19(2) Med Health Care and Philos 177
63. Sweeney L, 'A Model for Protecting Privacy' (2002) 10(5) IJUFKS 557
64. Taylor M, Taylor N, 'Health Research Access to Personal Confidential Data in England and Wales: Assessing Any Gap in Public Attitude Between Preferable and Acceptable Models of Consent' (2014)10 Life Science Society and Policy 15
65. Tierney W, Hui S, McDonald C, 'Delayed Feedback of Physician Performance Versus Immediate Reminders to Perform Preventive Care. Effects on Physician Compliance' (1986) 24(8) Med Care 659
66. Tierney W, McDonald C, Martin D, Hui S, Rogers M, 'Computerized Display of Past Test Results. Effect on Outpatient Testing' (1987) 107 Annals of Internal Medicine 569
67. Tierney W, Miller M and McDonald C, 'The Effect on Test Ordering of Informing Physicians of the Charges for Outpatient Diagnostic Tests' (1990) 322 NEJM 1499
68. Tierney W, Miller M, Overhage M and McDonald J, 'Physician Inpatient Order Writing on Microcomputer Workstations: Effects on Resource Utilization' (1993) 269(3) JAMA 379
69. Tonks A, 'Information Management and Patient Privacy in the NHS' (1993)307 BMJ 1227
70. Wang S, Middleton B, Prosser L, Bardon C, Spurr C, Carchidi P, Kittler A, Goldszer R, Fairchild D, Sussman A, Kuperman G, Bates D, 'A Cost-Benefit Analysis of Electronic Medical Records in Primary Care' [2003] (5) Am J Med 397, 114
71. Wanlass R, Reutter S and Kline A, 'Communication Among Rehabilitation Staff: "Mild", "Moderate" or "Severe" Deficits?' (1992) 73(5) Arch Phys Med Rehabil 477

72. Weed L, 'Medical Records That Guide and Teach' (1968) 278(11) NEJM 593
73. Weingarten S, Henning J, Badamgarak E, Knight K, Hasselblad V, Gano A, Ofman J, 'Interventions Used in Disease Management Programmes for Patients with Chronic Illness - Which Ones Work? Meta-Analysis of Published Reports' (2002) 325(7370) BMJ 925
74. Woods L, 'What Works: Scheduling. Picture Perfect Solution. The Right Technology and an ASP Solution Bring Scheduling Efficiency and Added Revenue to a Community Hospital's Radiology Department' (2001) 22(8) Health Manag Technol 48
75. Zurita L, Nohr, C, 'Patient Opinion: EHR Assessment from The Users' Perspective' (2004) 107(2) Stud Health Technol Inform 1333

Web Articles

1. Campion-Awward O, Alexander Hayton, Leila Smith and others, 'The National Programme for IT in the NHS: A Case History' (UOC 2014) <https://www.cl.cam.ac.uk/~rja14/Papers/npfit-mpp-2014-case-history.pdf> accessed on 3 Dec 2016.
2. HIMSS, CDS: Fundamental Issues < http://www.himss.org/library/clinical-decision-support/issues?navItemNumber=13240 > accessed on 9 December 2016
3. HIMSS, Electronic Health Records. <http://www.himss.org/library/ehr> accessed November 10, 2016.
4. Kontos E, Bennett G, Viswanath K, 'Benefits and Facilities to Home Computer and Internet Use Among Urban Novice Computer Users of Low Socioeconomic Position' (2009)9(4) J Med Internet Re e31 <http://www.jmir.org/2007/4/e31/> accessed on 1 January 2017.
5. NIH NCRR, Electronic Health Records Overview'2006. http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/Code%20180%20

MITRE%20Key%20Components%20of%20an%20EHR.pdf (accessed on 10 December 2016).

6. Powell J and Buchan I, 'Electronic Health Records Should Support Clinical Research' Journal of Medical Internet Research. 2005; 7(1): e4. <https://www.jmir.org/2005/1/e4/ >accessed on 16 January 2017.
7. Rivett G, National Health Service History < http://www.nhshistory.net > accessed on 10 January 2017.

Newspapers

1. Donnelly L, Britain's National Health Service: Medical Records Database "Raises Serious Privacy Issues — Patients deliberately kept in the dark"' Johnib Wordpress (17 February 2014) <https://johnib.wordpress.com/2014/02/17/britains-national-health-service-medical-records-database-raises-serious-privacy-issues-patients-deliberately-kept-in-the-dark/> accessed November 10, 2016.
2. Donnelly L, Hospital Records of all NHS Patients Sold to Insurers The Telehraph 23 February 2014 <http://www.telegraph.co.uk/news/health/news/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html > Accessed on 17 January 2017.
3. Ramesh R, NHS England Patient Data 'uploaded to Google server', Tory MP says The Guardian 3 March 2014 <https://www.theguardian.com/society/2014/mar/03/nhs-england-patient-data-google-servers > accessed on 07 January 2017.
4. Swinford S, Britain Considers Law To Protect Medical Records, Patient Data After National Service Sold Info To Insurers Johnib Wordpress, <http://johnib.wordpress.com/2014/03/01/britain-considers-law-to-protect-medical-records-patient-data-after-national-health-service-sold-info-to-insurers/> (accessed November 10, 2016).

Media

1. Big Brother Watch, NHS Breaches of Data Protection Law, (2001) <https://www.bigbrotherwatch.org.uk/files/NHS_Breaches_Data_Protection.pdf >Accessed on 3 January 2017.
2. Big Brother Watch, NHS Data Breaches (2014) <https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/11/EMBARGO-0001-FRIDAY-14-NOVEMBER-BBW-NHS-Data-Breaches-Report.pdf> Accessed on 3 January 2017
3. Department of Health Media Centre, *Leading expert launches review of NHS IT 8 February 2016* <https://healthmedia.blog.gov.uk/2016/02/08/bob-wachter/ > accessed on 10 January 2017.
4. Schneier B, The internet is a surveillance state (16 March 2013). <http://edition.cnn.com/2013/03/16/opinion/schneier-internet-surveillance > accessed on 6 January 2017