TRANSFoRm

Translational Research and Patient Safety in Europe

Report on regulatory requirements, confidentiality and data privacy issues

Part A: Regulatory requirements
(Deliverable 3.2)

Heinrich-Heine University Düsseldorf (UDUS), Coordination Centre for Clinical Trials on behalf of the European Clinical Research Infrastructures Network (ECRIN)

Quintiles

Work Package:	WP3, Deliverable 3.2
Type of document:	Conceptual framework
Version:	Version 1
Date:	31 March 2011
Authors:	C. Ohmann, W. Kuchinke (UDUS), H. Corley (Quintiles)

TRANSFoRm is partially funded by the European Commission - DG INFSO Under the 7th Framework Programme. (FP7 247787)
http://cordis.europa.eu/fp7/ict/
http://ec.europa.eu/information_society/index_en.htm

eHealth
Better Healthcare for Europe

European Commission
Information Society and Media

INDEX

Executive Summary

The objective of WT 3.1 on Regulatory Requirements is to detail the requirements of regulators for the development of clinical trial management software for publically funded clinical studies and randomised clinical trials of investigational medicinal products and for Diagnostic Decision Support Systems (where diagnostic predictions derived from knowledge of the patient's signs and symptoms are presented to the clinician to support diagnostic decision making).

To develop an in-depth analysis of the European regulatory requirements for Clinical Trial Data Management Systems (CDMS), the regulatory framework relating to clinical trials, software, electronic records and data protection was identified. This framework consists of European Regulations, Directives, guidance for industry, and other documents such as EMA reflection papers which shape the regulatory landscape. International guidelines, the ICH Topic on Good Clinical Practice and ISO standards were taken into account. Relevant USA regulations and guidance were also included, which is particularly important in the field of software and electronic records, where there is a lack of equivalent European guidance. The clinical research sector is also actively developing global standards and guidance documents for use in clinical research and these documents were included in the review.

The relationship of regulatory documents and directives to each other and to guidelines was mapped out by reviewing the references made within each document to other relevant documents. This ensures that all relevant documents have been identified. A matrix mapping the regulatory requirements to the corresponding CDMS requirement is provided. It details the regulatory documents which provide either general or specific requirements relating to data, data management and IT systems. This provides the basis for determining the user requirements for the CDMS for the purpose of system validation.

Although there is currently no recognised industry standard for specific CDMS system requirements, the European Clinical Research Infrastructure Network (ECRIN) has developed a standard describing the requirements of GCP-compliant data management in multinational clinical trials. This standard covers both the requirements for the IT infrastructure and computer systems in general, and the requirements for data management applications in clinical trials. International, European and national regulations and guidelines relevant to GCP, data security and IT infrastructures were considered in developing this standard. It therefore provides a set of user requirements for a CDMS which could be used to specify requirements for system validation of CDMS. Standards for CDMS system validation may be higher in some areas of clinical research than others, but will need to be taken into account for the TRANSFoRm project. Where the aim of clinical research is to bring new medicinal products to market, the use of electronic data and computerised systems to

produce the data in the marketing application must meet the requirements stipulated by the Regulatory Authorities and so will require CDMS system validation.

The use of electronic source data (eSource data) in clinical trials, where the data are captured in an electronic form rather than on paper is becoming increasing prevalent. There are a wide variety of data that may be generated electronically in the conduct of a clinical trial, such as electronic Case Report Forms (eCRF), laboratory test results, ECGs, X-rays and patient diaries. The ultimate desire is for single data capture and the interoperability of EHR with other systems such as Electronic Data capture (EDC). The current regulatory framework is still focussed on the use of paper source documents and paper-based processes rather than electronic source data and computer systems. However the recently published EMA Reflection paper and draft FDA guidance on eSource documentation are beginning to address this. Standards for eSource data are being developed, but are driven by different groups. In clinical research CDISC provide the direction. The CDISC eSDI Working Group has identified 12 user requirements that an eSource system must fulfil. In the healthcare sector, where Electronic Health Records (EHRs) are becoming more widely used, there are two organisations providing direction for the certification of EHR systems: Health Level 7 Inc., known as HL7 (an American standards development organization) and EuroRec (European Quality Labelling and Certification of Electronic Health Record), the European Union EHR certification committee. These organisations have jointly developed the Electronic Health Record for Clinical research (EHRCR) User requirements, which relate specifically to computerised EHRs used in Clinical Research and provide the core requirements for EHR systems to meet current regulations and guidance for clinical research.

Compliance with the regulations and guidance for clinical research, combined with the CDISC user requirements for eSource data, as detailed in the EMA Reflection Paper (regarding electronic source data) are necessary for regulatory acceptance of eSource data at present. eSource data taken directly from EHRs represent a greater challenge, since the EHR and system must meet clinical research standards. It is important to note that the European regulators are responding to the increasing use of computerised systems in clinical trials, with the recent issue of the EMA Reflection Paper regarding electronic source data (came into effect August 2010) and a revision to Good Manufacturing Practice Annex 11 regarding computerised systems (to come into operation on 30 June 2011). Annex 11 stipulates validation requirements and Good Clinical Practice (ICH E6 (R1)) requires validation of electronic data processing systems. It can therefore be expected that the regulatory landscape will continue to change for CDMS and electronic source data over the coming years.

1. Regulatory Requirements

1.1. Introduction

The regulatory framework governing medicinal products for human use in the European Union is made up of regulations, directives (that are transposed into national law), guidance documents from the European Medicines Agency (EMA) and national Regulatory Authorities, and international and European standards. In situations, such as the TRANSFoRm project, where this regulatory framework does not keep pace with healthcare and technological advances, draft standards, EMA reflection papers and industry guidance documents should be taken into consideration. Since the USA is a strong driver in the development of regulations that influence the European regulators, their regulations and guidance should also be taken into account.

The objective of WT 3.1 on Regulatory Requirements is to detail the requirements of regulators for the development of clinical trial management software for publically funded clinical studies and Randomised Clinical Trials (RCTs) of investigational medicinal products and for Diagnostic Decision Support Systems (where diagnostic predictions derived from knowledge about the predictive value of the patient's symptoms and signs are presented to the clinician to support diagnostic decision making). Therefore the regulatory framework relating to clinical trials, software, electronic records and data protection are reviewed in detail. In addition the industry guidance from the clinical research sector is reviewed.

Internet links to the documents, where available, are provided in Section 3 "References".

1.2. Listing of regulatory requirements for Clinical Trial Data Management Systems (CDMS)

1.2.1 General clinical trials

International, European and American regulatory documents specifying requirements for Clinical Trial Data Management Systems (CDMS) are summarised in Table 1.

1.2.2 Software and electronic records

International, European and National regulatory documents relating specifically to software and electronic record requirements are shown in Table 2.

1.2.3 Data protection

International, European and National regulatory documents relating to data protection requirements are shown in Table 3.

1.2.4 Clinical Research industry guidance documents

Stakeholders in clinical research are actively developing global standards in areas such as data standards to enable information system interoperability, and the functionality of Electronic Health Records (EHRs) for use in clinical research. These documents are detailed in Table 4.

1.3 Relationships between documents specifying requirements for CDMS

The references between the documents specifying requirements for CDMS are shown in Table 5. The type of references apply to the way in which a regulation or guideline is mentioned in the text of the corresponding document. Primary references are mentioned several times and are often explained in the text. Secondary references are only listed in a table or in the references chapter. How the different regulatory and guidance documents reference each other are shown in Figure 1.

Table 1: List of relevant documents from regulators specifying requirements for CTDMS used in clinical trials with medicinal products

Region	Reference/Title	Abbreviated reference	Description
International	ICH Topic E6 (R1): Guideline for Good Clinical Practice Step 5 CPMP/ICH/135/95	ICH E6 (R1)	*(see EMEA Note for Guidance on Good Clinical Practice)*
Europe	Directive 2001/20/EC: Implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use, 4 April 2004	EU 2001/20/EC	Directive 2001/20/EC establishes specific provisions regarding conduct of clinical trials, including multi-centre trials, on human subjects involving medicinal products, in particular to the implementation of good clinical practice
	Directive 2005/28/EC: principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products, 8 April 2005	EU 2005/28/EC	This Directive lays down the following provisions to be applied to investigational medicinal products for human use: the principles of good clinical practice and detailed guidelines in line with those principles, as referred to in Directive 2001/20/EC, for the design, conduct and reporting of clinical trials on human subjects involving such products; the requirements for authorisation of the manufacture or importation of such products and the detailed guidelines, provided for in Directive 2001/20/EC, on the documentation relating to clinical trials, archiving, qualifications of inspectors and inspection procedures.
	EMEA Note for Guidance on Good Clinical Practice, CPMP/ICH/135/95, July 2002	CPMP/ICH/135/95	Good Clinical Practice (GCP) is an international ethical and scientific quality standard for designing, conducting, recording and reporting trials that involve the participation of human subjects. Compliance with this standard provides public assurance that the rights, safety and well-being of trial subjects are protected, consistent with the principles that have their origin in the Declaration of Helsinki, and that the clinical trial data are credible. The objective of this ICH GCP Guideline is to provide a unified standard for the European Union (EU), Japan and the United States to facilitate the mutual acceptance of clinical data by the regulatory authorities in these jurisdictions. This guideline should be followed when generating clinical trial data that are intended to be submitted to regulatory authorities. The principles established in this guideline may also be applied to other clinical investigations that may have an

Region	Reference/Title	Abbreviated reference	Description
			impact on the safety and well-being of human subjects. Section 5.5.3 (electronic data handling and /or remote electronic data systems), Section 5.5.4 and Section 5.5.5 deal with data management.
USA	Guidance for Industry: E6 Good Clinical Practice: Consolidated Guidance (ICH April 1996)		*(see EMEA Note for Guidance on Good Clinical Practice)*
	FDA Guidance for Industry. Computerized Systems Used in Clinical Investigations (May 2007)	FDA CSUCI	This document provides to sponsors, contract research organizations (CROs), data management centers, clinical investigators, and institutional review boards (IRBs), recommendations regarding the use of computerized systems in clinical investigations. The computerized system applies to records in electronic form that are used to create, modify, maintain, archive, retrieve, or transmit clinical data required to be maintained, or submitted to the FDA. Because the source data are necessary for the reconstruction and evaluation of the study to determine the safety of food and color additives and safety and effectiveness of new human and animal drugs, and medical devices, this guidance is intended to assist in ensuring confidence in the reliability, quality, and integrity of electronic source data and source documentation (i.e., electronic records). The guidance supplements the guidance for industry on Part 11, Electronic Records; Electronic Signatures — Scope and Application.
	Good Clinical Data Management Practice, Version 4, Society for Clinical Data Management, October 2005.		The Good Clinical Data Management Practices (GCDMP) guide provides assistance to clinical data managers in their implementation of high quality clinical data management processes and is used as a reference tool for clinical data managers when preparing for CDM training and education. The GCDMP is now available, by chapter, from the Society for Clinical Data Management (SCDM) membership The GCDMP is an electronic text of best practices for clinical data management. Chapters are added and revised regularly to keep the document up-to-date with the most recent standards

Table 2: List of regulatory documents relating specifically to software and electronic record requirements

Region	Reference/Title	Abbreviated reference	Description
Inter-national	ISO 27001: Information Security Management – Specification with Guidance for Use Not available for free download	ISO 27001	Standard ISO 27001, titled "Information Security Management - Specification With Guidance for Use", is the replacement for the original document, BS7799-2. It is intended to provide the foundation for third party audit, and is 'harmonized' with other management standards, such as ISO 9001 and ISO 14001. The basic objective of the standard is to help establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organization for Economic Cooperation and Development) principles, governing security of information and network systems.
Europe	GCP Inspectors Working Group: Reflection paper on expectations for electronic source documents used in clinical trials. Effective date: 1 August 2010. Ref. EMA/INS/GCP/454280/2010	GCP Inspectors WG	This reflection paper sets out the current thinking of the EU GCP Inspectors Working Group on the use of electronic source documents and data in clinical trials and on the inspection of these. The document is based around the 12 user requirements stated in the CDISC document on electronic source records.
	EudraLex - The Rules Governing Medicinal Products in the European Union. Volume 4 - Good Manufacturing Practice, Medicinal products for human and veterinary use. Annex 11 - Computerized Systems' Revision 1 issued January 2011 and comes into effect on 30 June 2011	Eudralex V4 Annex 11	This annex applies to all forms of computerised systems used as part of GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities. The application should be validated; IT infrastructure should be qualified. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.
USA	Electronic Records, Electronic Signatures Final Rule (21 CFR Part 11, 20-Mar-1997)	FDA CFR 21 (11)	The regulation defines criteria for electronic records, electronic signatures, and handwritten signatures to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.
	FDA Guidance for Industry. Part 11, Electronic Records; Electronic	FDA Guidance Part 11	This guidance is intended to describe the Food and Drug Administration's (FDA's) current thinking regarding the scope and application of part 11 of Title 21 of the Code

Region	Reference/Title	Abbreviated reference	Description
	Signatures – Scope and Application (August 2003)		of Federal Regulations; Electronic Records; Electronic Signatures (21 CFR Part 11). This document provides guidance to persons who, in fulfillment of a requirement in a statute or another part of FDA's regulations to maintain records or submit information to FDA have chosen to maintain the records or submit designated information electronically and, as a result, have become subject to part 11.
	FDA Guidance for Industry. Computerized Systems Used in Clinical Investigations (May 2007)	FDA CSUCI	The principles outlined in this guidance should be used for computerized systems that contain any data that are relied on by an applicant in support of a marketing application, including computerized laboratory information management systems that capture analytical results of tests conducted during a clinical trial. For example, the recommendations in this guidance would apply to computerized systems that create source documents (electronic records) such as case histories. This guidance also applies to recorded source data transmitted from automated instruments directly to a computerized system (e.g., data from a chemistry autoanalyser or a Holter monitor to a laboratory information system). This guidance also applies when source documentation is created in hardcopy and later entered into a computerized system, recorded by direct entry into a computerized system, or automatically recorded by a computerized system (e.g., an ECG reading).
European National			
Denmark	Implementation of Good Clinical Practice Software, Lauritsen J M, University of Southern Denmark (02/2007, Draft)		National document on regulatory requirements
Germany	German Coordinating Centres for Clinical Trials networks Policy Document (October 23rd 2001, updated December 20th 2007)		National document on regulatory requirements
UK	Data and Information Management Systems Project - System Standards - UKCRC / NIHR (2009)		National document on regulatory requirements

Region	Reference/Title	Abbreviated reference	Description
Germany	IT-Grundschutz Methodology, Bundesamt für Sicherheit in der Informationstechnik (BSI).		National document on regulatory requirements

Table 3: List of relevant documents from regulators relating to data protection

Region	Reference/Title	Description
Europe	**Directive 95/46/EC** of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	Directive 95/46/EC protects fundamental rights and freedom of natural persons, and in particular their right to privacy with respect to the processing of personal data. The Directive says nothing on medical research explicitly. Its implications for the processing of personal data in/for medical research must be inferred from what it has to say about the general processing of personal data, especially sensitive personal data, and about processing for research and statistics. For this reason, the following outline does not mention medical research specifically unless this can be done without distorting the provisions of the Directive
	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)	(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community. (2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter. (3) Confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms, and the constitutions of the Member States. (10) In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.
	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks	(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3] requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community. (5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably. (6) The legal and technical differences between national provisions concerning the retention of data for the

Region	Reference/Title	Description
	and amending Directive 2002/58/EC, OJ L 105 13.04.2006 p. 54	purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention. (13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.
	Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data	(1) Article 286 of the Treaty requires the application to the Community institutions and bodies of the Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data. (2) A fully-fledged system of protection of personal data not only requires the establishment of rights for data subjects and obligations for those who process personal data, but also appropriate sanctions for offenders and monitoring by an independent supervisory body. (7) The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever, for example because they are employed by those institutions or bodies. (8) The principles of data protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely to be reasonably used either by the controller or by any other person to identify the said person. The principles of protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.
	Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Official Journal L 350, 30.12.2008 P. 0060 – 0071	(1) The European Union has set itself the objective of maintaining and developing the Union as an area of freedom, security and justice in which a high level of safety is to be provided by common action among the Member States in the fields of police and judicial cooperation in criminal matters. (2) Common action in the field of police cooperation under Article 30(1)(b) of the Treaty on European Union and common action on judicial cooperation in criminal matters under Article 31(1)(a) of the Treaty on European Union imply a need to process the relevant information which should be subject to appropriate provisions on the protection of personal data. (6) This Framework Decision applies only to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
	Directive 97/66/EC of the European Parliament and of the Council of 15	(1) Whereas Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such

Region	Reference/Title	Description
	December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector	data (4) requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community; (2) Whereas confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights (in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms) and the constitutions of the Member States; (3) Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterised by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk; (12) Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider necessary for the protection of public security, defense, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;
	Treaty on the European Union (TEU)	Article 6 1. The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions. 2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties. 3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.
	European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)	Article 8 – Right to respect for private and family life Everyone has the right to respect for his private and family life, his home and his correspondence. 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

Region	Reference/Title	Description
		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.
	EU Charter of Fundamental Rights of 7 December 2000	Article 8: Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority. Article 41: the right of every person to have access to his or her file, while respecting the legitimate interests of confidentiality and of professional and business secrecy;
	Commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC	Article 1 The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive 95/46/EC. STANDARD CONTRACTUAL CLAUSES (PROCESSORS): The parties HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.
	Case law C-518/07 European Court of Justice: C-518/07. European Commission supported by European Data Protection Supervisor vs. Federal Republic of Germany (judgement of 9 March 2010) / Failure of a Member State to fulfil obligations – Directive 95/46/EC – Protection of individuals with regard to the processing of personal data and the free movement of such data – Article 28(1) – National supervisory authorities – Independence – Administrative scrutiny of those authorities.	Judgment of the Court (Grand Chamber) of 9 March 2010. European Commission vs. Federal Republic of Germany (Case C-518/07). Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data There is therefore a difference between the authorities responsible, on the one hand, for monitoring compliance with the provisions concerning data protection by public bodies and, on the other hand, for monitoring compliance with data protection by non-public bodies and undertakings governed by public law which compete on the market (öffentlich-rechtliche Wettbewerbsunternehmen) ('outside the public sector'). The processing of data by public bodies is supervised, at Federal level, by the Federal representative responsible for the protection of personal data and freedom of information ('Bundesbeauftragter für den

Region	Reference/Title	Description
		Datenschutz und die Informationsfreiheit') and, at regional level, by the representatives responsible for the protection of regional data ('Landesdatenschutzbeauftragte'). Those representatives are solely responsible to their respective parliament and are not normally subject to any scrutiny, instruction or other influence from the public bodies which are the subjects of their supervision.
	Status of implementation of Directive 95/46 Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data.	The table contains descriptions of situation in Member States
	Promoting Data Protection by Privacy Enhancing Technologies (PETs) Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), Brussels, 2.5.2007	Several examples of PETs can be mentioned: Automatic anonymisation of data, after a certain lapse of time, supports the principle that processed data should be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the data were originally collected. Encryption tools, preventing hacking when information is transmitted over the Internet, support the data controller's obligation to take appropriate measures to protect personal data against unlawful processing. Cookie-cutters, that block cookies placed on the user's PC to make it perform certain instructions without the user being aware of them, enhance compliance with the principle that data must be processed fairly and lawfully, and that the data subject must be informed about the processing going on. The Platform for Privacy Preferences (P3P), allowing internet users to analyze the privacy policies of websites and compare them with the user's preferences as to the information they wish to release, helps to ensure that data subjects' consent to processing of their data is an informed one. The Commission considers that PETs should be developed and more widely used, in particular where personal data is processed through ICT networks. The Commission considers that wider use of PETs would improve the protection of privacy as well as help fulfill data protection rules. The use of PETs would be complementary to the existing legal framework and enforcement mechanisms. The intervention of different actors in data processing and the existence of different national jurisdictions involved could make enforcement of the legal framework difficult. On the other hand, PETs could ensure that certain breaches of data protection rules, resulting in invasions of fundamental rights including privacy, could be avoided because they would become technologically more difficult to carry out.
	Declaration of Helsinki, 2008 WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects, 59th WMA	The World Medical Association (WMA) has developed the Declaration of Helsinki as a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data. PRINCIPLES FOR ALL MEDICAL RESEARCH 11. It is the duty of physicians who participate in medical research to protect the life, health, dignity,

Region	Reference/Title	Description
	General Assembly, Seoul, October 2008	integrity, right to self-determination, **privacy, and confidentiality of personal information of research subjects**. 23. Every precaution must be taken to protect the **privacy of research subjects and the confidentiality of their personal information** and to minimize the impact of the study on their physical, mental and social integrity.
European National		
France	Méthodologie de Référence – MR001 (Benchmark standards for personal data processing in GCP-clinical trials). Published by the French Data Protection Authority - Commission national de l'informatique et des libertés (CNIL)	This is a voluntary scheme to which companies can self-certify as compliant, following which they are exonerated from prior authorization submissions
Italy	Guidelines for Data Processing within the Framework of Clinical Drug Trials - 24 July 2008 Published by the Italian Data Protection Authority "GARANTE"	
Spain	Standards for clinical trial personal data processing	Published by the Spanish Pharmaceutical Industry "farmaindustrie". Like the French Méthodologie, it promotes self-regulation to a set of standards.
Ireland	Data Protection Guidelines on Research in the Health Sector November 2007	Guidelines issued by the Irish Data Protection Authority
Denmark	The personal data act, clinical trials and data privacy. Rules for treatment of personal data in clinical trials and scientific research projects.	Published by the Danish Data Protection Authority.
UK	Use and Disclosure of Health Data. May 2002.	Published by the UK Data Protection Authority "Information Commission

Region	Reference/Title	Description
	Guidance on the Application of the Data Protection Act 1998	

Table 4: Healthcare and Clinical Research guidance documents

Reference/Title/Web address	Description
The eClinical Forum and PhRMA EDC/eSource Taskforce (2006): The future vision of electronic health records as eSource for clinical research. Version 1.0, 14 September 2006	The document offers a future vision of how patient data, already collected by physicians and entered into electronic systems, might be leveraged for clinical research in conjunction with trial-specific data collected in the same efficient and regulatory-compliant manner thus benefiting healthcare professionals, patients, regulatory authorities and sponsors of clinical trials.The eClinical Forum (formerly the Electronic Data Management Forum) is a transatlantic, not-for-profit and non-commercial, technology independent group representing members of the pharmaceutical, biotechnology, and allied industries.
Clinical Data Interchange Standards Consortium, Electronic Source Data Interchange (eSDI) Group (): Leveraging the CDISC Standards to Facilitate the use of Electronic Source Data within Clinical Trials. Version 1.0, 20 November 2006	This document is intended to align multiple factors in the current global regulatory environment to encourage the use of electronic source data (eSource) collection and industry data standards to facilitate clinical and biomedical research for investigators, sponsors and other stakeholders. The document includes a mapping to technology and a mapping to regulatory text (ICH GCP, CSUCT). This document is intended to align multiple factors in the current global regulatory environment to encourage the use of electronic source data (eSource) collection and industry data standards to facilitate clinical and biomedical research for investigators, sponsors and other stakeholders.
Pharmaceutical Inspection Convention, PIC/S Guidance: Good practices for computerized systems in regulated “GXP” environments, 25 September 2007	The PIC/S Guide to Good Manufacturing Practices is the basis for GMP Inspections. The purpose of this document is to provide recommendations and background information concerning computerised systems that will be of assistance to inspectors for training purposes and during the inspection of computerized systems.
Electronic Health Records for Clinical Research (EHRCR) Working Group (2010): Practical considerations for clinical trial sites using electronic health records (EHRs) in support of clinical research. Addressing regulatory considerations. Release 1.0, January 18, 2010	This document is intended as a practical guide to assist clinical research site personnel in: understanding and anticipating expectations when participating in clinical research (regardless of whether they are using an EHR system), selecting or upgrading an EHR system to hold data which could potentially become source data to support regulated research work for drug or medical device clinical trials or development activities and identifying best practices in implementing and maintaining an EHR system, especially if it may hold data that could become source for clinical trials. A checklist is provided to identify site activities in selecting and implementing EHR. The document refers to FDA 21 CFR Part 11 and Part 312, ICH GCP, EU annex11, EU Directives 2001/20 and 2005/28, FDA CSUCI and US HIPAA. The Electronic Health Record for Clinical Research (EHRCR) Project was organized in December 2006 at the invitation of the Health Level Seven (HL-7) Technical Committee and EuroRec (see Appendix 2, References, Section 4 and 5). The project objective was to define requirements to expand and adapt the functionality of EHR technologies, including the associated systems, networks, and processes, in order to support the needs of regulated clinical research.

Reference/Title/Web address	Description
EHRCR Functional Profile Working Group, eClinicalForum and PhRMA EDC/eSource Task Force: EHRCR User requirements Document, January 2010	This User Requirements document clarifies the minimum requirements to use healthcare systems as the data source for regulated clinical research today, in order to ensure the reliability of clinical research data from EHR (Electronic Health Record) systems. These User Requirements have been mapped to regulations and guidance documents, and to the final approved HL7 normative version of the EHRCR Functional Profile (which has undergone extensive stakeholder scrutiny), and to the EuroRec EHRCR profile. The document refers to FDA, ICH GCP, EU Annex11, EU Directives, FDA CSUCI and US HIPAA.
EHRCR Working Group: Electronic Health Records/Clinical Research: EuroRec Electronic Health Records for Clinical Research Functional Profile, Version 1.0 January 2010	This document describes a Functional profile that identifies critical capabilities for the conduct of regulated clinical research using EHR systems. The use of this EHRCR Functional profile will ensure that data protection, patient privacy and regulatory research requirements are met. The document refers to organisations working in this field, such as CCHIT, CDISC and EuroRec. It refers to regulatory requirements ICH GCP, ISO/TR 20514 and US HIPAA and FDA 21 CFR Part 11 and Guidance for Industry documents.
Clinical Data Acquisition: Standards Harmonization (CDASH), CDASH_STD-1.0, 01/OCT/2008	The Clinical Data Acquisition Standards Harmonization (CDASH) Standard Version 1.0 describes recommended basic standards for the collection of clinical trial data. The CDASH standards are part of the Clinical Data Interchange Standards Consortium (CDISC) Technical Road Map that is designed to realize the vision of a set of harmonized standards that meet the CDISC Mission and Strategy. The set of standards has been, and will continue to be, developed to support the streamlining of processes within medical research from the production of clinical research protocols through to reporting and/or regulatory submission, warehouse population and/or archive and post-marketing studies/safety surveillance. The document refers to the Code of Federal Regulations (CFR); European Commission directives; ICH Harmonized Efficacy Guidelines finalized as of 14 March 2008; FDA Guidances finalized as of 14 March 2008; FDA Manual of Policies and Procedures; Compliance Program Guidance Manual and NCI Code lists.
European Clinical Research Infrastructures Network (ECRIN) and Biotherapy Facilities: Preparation Phase for the Infrastructure: Standard requirements for GCP-compliant data management in multinational clinical trials; Ref. ECRIN-PPI No. 211738	This document describes the requirements of GCP-compliant data management in multinational clinical trials, which covers both the requirements for the IT infrastructure and computer systems in general, and the requirements for data management applications in clinical trials. The standard covers 115 IT-requirements, 107 data management requirements and 13 other requirements. It is intended to be widely used, but particularly in academic trial units (*see publication: Ohmann C et al.: Standards requirements for GCP-compliant data management in multinational clinical trials. Trials 2011; 12:85)*

Table 5: References between documents specifying requirements for CTDMS

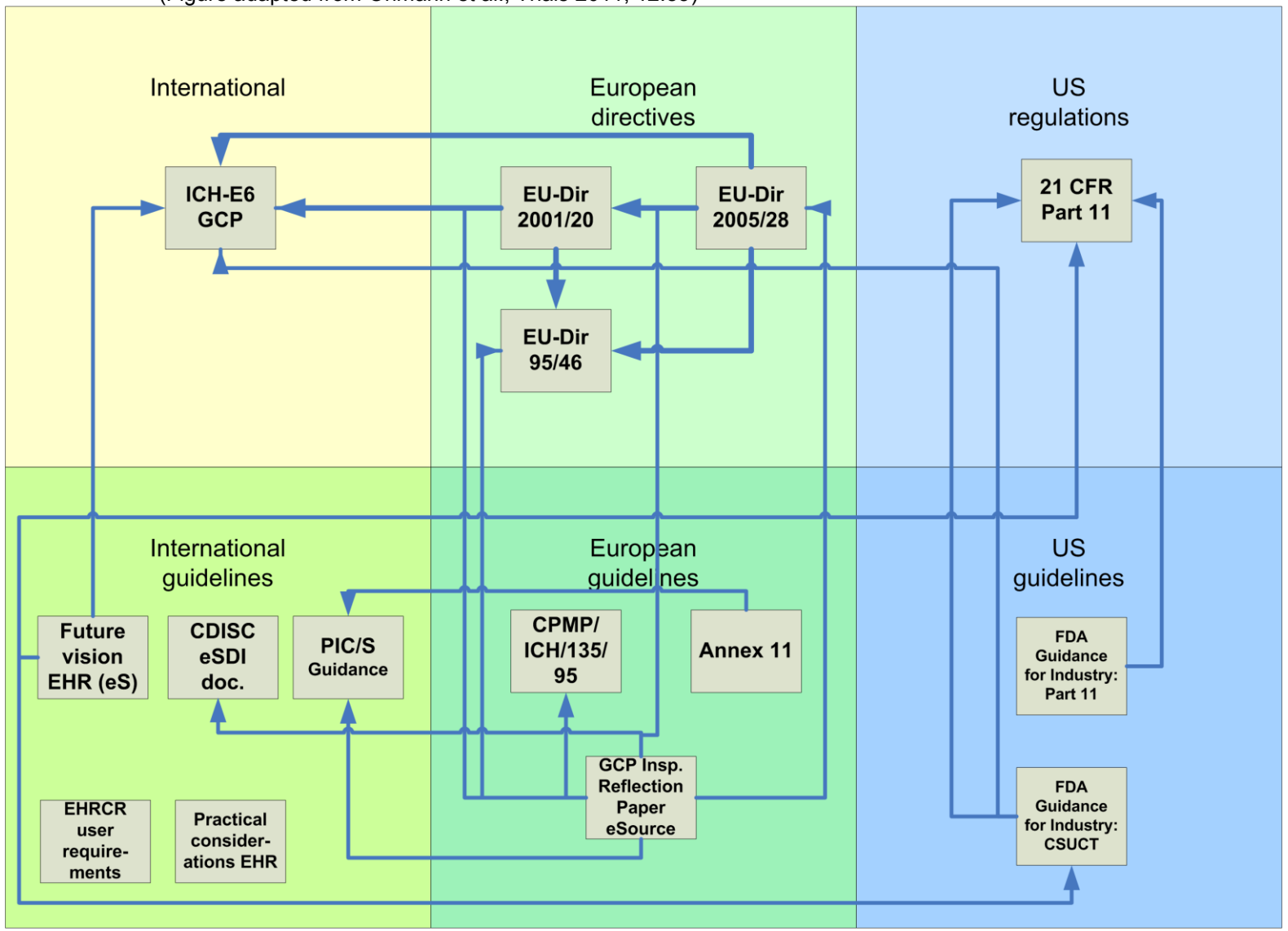
Nr.	Document				References	
	title	authoring	year	status	primary	secondary
1	ICH-E6 GCP guideline	ICH Expert Working Group, consultations by regulatory bodies	1996	International guideline of the ICH for adoption by regulatory bodies in EU, US and Japan.	Declaration of Helsinki	
2	CPMP/ICH/135/95	Corresponds to 1	2002	Guideline of the EMA for Europe. Agreed upon by CHMP of the EMA	Declaration of Helsinki	
3	2001/20/EC	EU Directive by the European parliament and of the Council,	2001	Directive addressed to the member states for implementation. Member states shall adopt laws and regulations to comply with the directive.	Good Clinical Practice Declaration of Helsinki	Directive 65/65/EEC Directive 95/46/EC Directive 91/356/EEC
4	2005/28/EC	EU Directive by the EU commission	2005	Directive addressed to the member states for implementation. Member states shall adopt laws and regulations to comply with the directive	Good Clinical Practice Ethical Principles by WHO 2001/20/EC	2003/94/EC 2001/83/EC Directive 95/46/EC
5	Directive 95/46/EC	EU Directive by the European parliament and of the Council	1995	Directive addressed to the member states for implementation. Member states shall adopt laws and regulations to comply with the directive	Treaty on the European Union European Convention for the Protection of Human Rights Community law	Council decision 87/373/EEC
6	GCP Inspectors Working Group: Reflection paper on expectations for electronic source documents used in clinical trials	GCP Inspectors Working Group of EMA	2010	. The reflection paper outlines the current opinion of the EU GCP Inspectors Working Group on the use of electronic data capture in clinical trials and on related inspections	Good Clinical Practice CPMP/ICH/135/95 Directive 95/46/EC CDISC e-SDI publication 2001/20/EC 2005/28/EC	ICH E6
7	Annex 11, EudraLex / Vol-4	European Commission Enterprise	2008	Guidance document, supplementary to the EU GMP Guide		GMP Annex 15 PIC/S Guidance GMP Guide Chap.4 ISO 17799

Nr.	Document				References	
	title	authoring	year	status	primary	secondary
8	21 CFR Part11	FDA	1997,	Code of Federal Regulations		62 FR 13464
9	Guidance for industry, Part11	CDER of FDA	2003	Nonbinding recommendations. It represents the agency's current thinking about the application of Part11	21 CFR Part11 Federal Food, Drug and Cosmetic Act Public Health Service Act	62 FR 13430 21 CFR Part 211 21 CFR Part 820 21 CFR Part 58 68 FR 8775 General principles of SW validation (FDA, 2002) Guidance for industry on Off-the-shelf software (1999) Pharmaceutical CGMPs (FDA 2002) GAMP4 ISO/IEC 17799:2000 ISO 14971:2002
10	Guidance for industry, Computerized Systems	US Dep of Health and Human Services and FDA	1999, 2007	Nonbinding recommendations. It represents the FDA's current thinking on the topic	21 CFR Part11 ICH-E6 GCP 21 CFR 812 21 CFR 11.10	21 CFR 312 FDA Compliance Policy Guide 7150.13 FDA Compliance Program Guidance Manual General principles of SW validation (FDA, 2002)
11	Future Vision of EHR as eSource	eClinical Forum/ PhRMA team	2006	Discussion document	PhRMA IMPACC paper (2005) 21 CFR Part11 21 CFR 312.62 (b) Guidance for industry, Computerized Systems (2004) ICH-E6 GCP	Guidance for industry, Computerized Systems (1999) HIPAA Guidance on PRO (FDA 2006) 45 CFR Part 46 45 CFR Part 160, 164

Nr.	Document				References	
	title	authoring	year	status	primary	secondary
12	Leveraging the CDISC standard for eSource	eSDI group of CDISC	2006	Recommendations for industry and FDA	21 CFR 312 21 CFR Part11 ICH-E6 GCP Guidance for industry, Computerized Systems (1999)	Guidance for industry, Part11 (2003) FDA Guidance for Regulatory Submission (eCTD) ICH E9 21 CRF Parts 50, 56, 511, 812 2001/20/EC 2005/28/EC HIPAA
13	PIC/S Guidance	Pharmaceutical Inspection Convention	2007	Recommendations for computerised systems for GXP inspections, adopted by the PIC/S Committee	GMP Annex 11 GAMP 4 ISO9000 ISO/IEC 12207:1995 21 CFR Part11	ISO 15504 Final guidance for industry and FDA Stuff: Software Validation (2002) GMP Annex15 ISO9004 ISO9126 ISO10005 ISO10007 IEEE 829 IEEE 1298 ISO 9126 BS 7799:1999 “Code of practice for information security management”: BSI/DISC Directive 2001/83 Directive 1999/93/EC Directive 2000/31/EC Directive 91/356/EEC German AVP

Nr.	Document				References	
	title	authoring	year	status	primary	secondary
14	Practical considerations using EHR	EHRCR working group (eClinical Forum and PhRMA eS-TG)	2010	Recommendations for clinical research site personnel	21 CFR Part11 21 CFR Part312 ICH-GCP GMP Annex11 2001/20/EC 2005/28/EC Guidance for industry, Computerized Systems	HIPAA Future Vision of EHR as eSource Directive 95/26/EC Directive 2002/58/EC US HITSP EHRCR functional profile CDISC CDASH 21 CFR 312 Directive 2001/83/EC Directive 2003/94/EC EU Regulation 1902/2006 45 CFR 160, 164 Directive 95/46/EC Directive 2002/58/EC 21 CFR Part 50, 54, 56, 314 CDISC eSDI document
15	EHRCR User Requirements Document	EHRCR FP working group (eClinical Forum and PhRMA eS-TG)	2010	User requirements	Guidance for industry, Computerized Systems 21 CFR Part11 HIPAA CDISC eSDI document ICH-GCP 2001/20/EC 2005/28/EC GMP Annex11	21 CFR Part312, 511, 812 CDISC CDASH

Figure 1: References of regulatory documents and directives to each other and to guidelines
(Figure adapted from Ohmann et al., Trials 2011; 12:85)



1.4 Mapping of regulatory requirements to CDMS specifications

A matrix mapping the regulatory requirements to the corresponding CDMS requirement are shown in Table 6. This table shows the regulatory documents which provide either general or specific requirements relating to data, data management and IT systems. This provides the basis for determining the user requirements for the CDMS for the purpose of system validation. (This approach is based on that used by the EHRCR Functional Profile Working group[1] to produce the user requirements for Electronic Health Records (EHR) where EHRs are the data source for clinical research. These user requirements provide the specific system requirements).

Unfortunately there is currently no industry standard for CDMS providing the specific system requirements. The European Clinical Research Infrastructure Network (ECRIN) has developed a standard describing the requirements of GCP-compliant data management in multinational clinical trials, which covers both the requirements for the IT infrastructure and computer systems in general, and the requirements for data management applications in clinical trials. International, European and national regulations and guidelines relevant to GCP, data security and IT infrastructures were considered in developing this standard. It therefore provides a set of user requirements for a CDMS which could be used to define the system validation of CDMS.

1.5 System validation of CDMS

It is important to note that the European regulators are responding to the increasing use of computerised systems in clinical trials, with the recent issue of an EMA Reflection Paper regarding electronic source data (came into effect August 2010) and a revision to Good Manufacturing Practice Annex 11 regarding computerised systems (to come into operation on 30 June 2011). Annex 11 stipulates validation requirements and Good Clinical Practice (ICH E6 (R1)) requires validation of electronic data processing systems. The FDA also has guidance documents on computerised systems used in clinical investigations and the use of electronic records and electronic signatures.

Standards for system validation may be higher in some areas of clinical research than others, but will need to be taken into account for the TRANSFoRm project. Where the aim of clinical research is to bring new medicinal products to market, the use of electronic data and computerised systems to produce the data in the marketing application must meet the requirements stipulated by the Regulatory Authorities and so will require CTDMS system validation.

[1] EHRCR Functional Profile Working Group, eClinicalForum and PhRMA EDC/eSource Task Force: EHRCR User requirements Document, January 2010

The ECRIN standard (described in Section 1.4), which is aimed in particular at academic clinical trial units, provides specific requirements with respect to validation (Ohmann et al., Trials 2011; 12:85):

IT06. General IT System Validation

ID	*Cat.*	*Requirement*
IT06.01	*min*	*Validation Policies:* Policies and SOPs should be in place covering system validation systems and processes
IT06.02	*min*	*Validation master plan:* The unit should have a validation master plan in place, identifying systems, the risks associated with each, and the consequent validation strategy for each
IT06.03	*min*	*Risk based approach:* The general approach to validation of any system should be based on analysis of potential risk, and take into account the system's usage, users and origins
IT06.04	*min*	*Individual validation plans:* Detailed validation plans should exist for any particular system, in line with the master plan and policies described above, detailing the validation required, how and when it should be done, and how it should be recorded
IT06.05	*min*	*Summaries and Recording:* A signed and dated summary of the results of each major validation episode should exist, for each system being validated
IT06.06	*min*	*Detailed Evidence:* More detailed evidence - e.g. of test results or signed user statements - should be available as evidence for the summary validation documents
IT06.07	*min*	*Change Control Policies:* Policies and SOPs should be in place defining change control mechanisms and their scope, who should authorise and review requests, and how they should be documented.
IT06.08	*min*	*Change and Re-validation:* Changes in systems should result in a review of the need for revalidation
IT06.09	*min*	*Software Development:* Evidence should be available that QA processes during software development have been implemented properly

DM 02: Clinical data management application - Validation

No.	*Cat.*	*Requirement*
DM02.01	*min*	**Clinical Data Management Application** *Policies*: SOPs and policies for **clinical data management application** and CDMS validation are in place
DM02.02	*min*	*Trial-specific Test Plan*: A trial-specific test plan defines the test methodology, covering scope of test, item pass/fail criteria, etc.
DM02.03	*min*	*Test against Functional Specifications*: The testing with sample data against functional specifications is carried out before deployment to live environment
DM02.04	*min*	*Test of Data Checks*: tests of all validation checks and conditional data capture mechanisms, plus any derivations are conducted, documented and retained
DM02.05	*min*	*Validation Report*: data validation final report for the trial has to be provided and signed by responsible DM person
DM02.06	*min*	*CRF Approval*: approval of the CRF is signed off by key persons
DM02.07	*min*	*Check of Validation Programs, Lists and Scripts*: validation programs, lists and scripts are checked, tested, documented and retained
DM02.08	*bp*	*Validation against Specifications:* the process of **clinical data management application** design and data checks programming is validated against specifications
DM02.09	*bp*	*Validation Report Generation*: system is able to generate reports used for validation

To meet the needs of both academic and commercial clinical research, it may be possible to take a risk management approach to system validation for TRANSFoRm as described in GMP Annex11:

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, ***decisions on the extent of validation and data integrity controls*** *should be based on a justified and documented risk assessment of the computerised system*.

Table 6: Regulatory requirements for the development of Clinical Data Management Systems (CDMS)

Abbreviated Reference of Regulation/Guidance	Section	Description
ICH E6 (R1) and CPMP/ICH/135/95	2.10	All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification.
	2.11	The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s).
	4.9.3	Any change or correction to a CRF should be dated, initialed, and explained (if necessary) and should not obscure the original entry (i.e. an audit trail should be maintained); this applies to both written and electronic changes or corrections (see 5.18.4 (n)). Sponsors should provide guidance to investigators and/or the investigators' designated representatives on making such corrections. Sponsors should have written procedures to assure that changes or corrections in CRFs made by sponsor's designated representatives are documented, are necessary, and are endorsed by the investigator. The investigator should retain records of the changes and corrections.
	4.9.4	The investigator/institution should maintain the trial documents as specified in Essential Documents for the Conduct of a Clinical Trial (see 8.) and as required by the applicable regulatory requirement(s). The investigator/institution should take measures to prevent accidental or premature destruction of these documents.
	4.9.5	Essential documents should be retained until at least 2 years after the last approval of a marketing application in an ICH region and until there are no pending or contemplated marketing applications in an ICH region or at least 2 years have elapsed since the formal discontinuation of clinical development of the investigational product. These documents should be retained for a longer period however if required by the applicable regulatory requirements or by an agreement with the sponsor. It is the responsibility of the sponsor to inform the investigator/institution as to when these documents no longer need to be retained (see 5.5.12).
	4.9.7	Upon request of the monitor, auditor, IRB/IEC, or regulatory authority, the investigator/institution should make available for direct access all requested trial-related records.
	5.5.3	When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should: (a) Ensure and document that the electronic data processing system(s) conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. validation). (b) Maintains SOPs for using these systems. (c) Ensure that the systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e. maintain an audit trail, data trail, edit trail). (d) Maintain a security system that prevents unauthorized access to the data. (e) Maintain a list of the individuals who are authorized to make data changes (see 4.1.5 and 4.9.3). (f) Maintain adequate backup of the data. (g) Safeguard the blinding, if any (e.g. maintain the blinding during data entry and processing).
	5.5.4	If data are transformed during processing, it should always be possible to compare the original data and observations

Abbreviated Reference of Regulation/Guidance	Section	Description
		with the processed data.
	5.5.5	The sponsor should use an unambiguous subject identification code (see 1.58) that allows identification of all the data reported for each subject.
EU 2001/20/EC	(16)	The person participating in a trial must consent to the scrutiny of personal information during inspection by competent authorities and properly authorised persons, provided that such personal information is treated as strictly confidential and is not made publicly available.
EU 2005/28/EC	Article 5	All clinical trial information shall be recorded, handled, and stored in such a way that it can be accurately reported, interpreted and verified, while the confidentiality of records of the trial subjects remains protected.
	Article 17	The sponsor and the investigator shall retain the essential documents relating to a clinical trial for at least five years after its completion. They shall retain the documents for a longer period, where so required by other applicable requirements or by an agreement between the sponsor and the investigator. Essential documents shall be archived in a way that ensures that they are readily available, upon request, to the competent authorities. The medical files of trial subjects shall be retained in accordance with national legislation and in accordance with the maximum period of time permitted by the hospital, institution or private practice.
	Article 20	The media used to store essential documents shall be such that those documents remain complete and legible throughout the required period of retention and can be made available to the competent authorities upon request. Any alteration to records shall be traceable.
EU 95/46/EC	(29)	Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;
	(30)	Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;
	(33)	Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly

Abbreviated Reference of Regulation/Guidance	Section	Description
		provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;
	(34)	Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;
	(38)	Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;
	(39)	Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;
	(40)	Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;
	(46)	Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;
	(48)	Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;
	(49)	Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the

Abbreviated Reference of Regulation/Guidance	Section	Description
		controller, must be in a position to exercise his functions in complete independence;
Eudralex V4 Annex 11	1	Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.
	3.1	When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.
	3.2	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.
	3.3	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.
	3.4	Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.
	4	***Validation***
	4.1	The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.
	4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.
	4.3	An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.
	4.4	User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.
	4.5	The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.
	4.6	For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.
	4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.
	4.8	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.
	5	***Data:*** Computerised systems exchanging data electronically with other systems should include appropriate built-in

Abbreviated Reference of Regulation/Guidance	Section	Description
		checks for the correct and secure entry and processing of data, in order to minimize the risks.
	6	***Accuracy Checks:*** For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.
	7	***Data Storage***
	7.1	Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.
	7.2	Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.
	8.1	It should be possible to obtain clear printed copies of electronically stored data.
	9	***Audit Trails:*** Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.
	10	***Change and Configuration Management:*** Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.
	11	***Periodic evaluation:*** Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.
	12	***Security***
	12.1	Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.
	12.2	The extent of security controls depends on the criticality of the computerised system.
	12.3	Creation, change, and cancellation of access authorisations should be recorded.
	12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.
	13	***Incident Management:*** All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.
	14	***Electronic Signature:*** Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.
	16	***Business Continuity:*** For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or

Abbreviated Reference of Regulation/Guidance	Section	Description
		alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.
	17	***Archiving:*** Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.
GCP Inspectors WG	4. SCOPE	This reflection paper is aimed primarily at the instruments, software and services provided by the sponsors or their contractors. The scope of this reflection paper is electronic systems, (including instruments, software and services) used in clinical trials in the creation/capture of electronic clinical data, such as: - Electronic Case Report Forms (e-CRFs) e.g. laptop/desktop, mobile device based programs or web based tools, which may contain source data directly entered, transcribed data by re-keying from other sources, or both. - Electronic patient data capture devices used to collect Patient Reported Outcome (PRO) data– e.g. mobile devices supplied to patients to record observations, rating scales, IMP use. This can be primary efficacy or supportive data. - Instruments supplied to investigators for recording clinical data either by data entry or by automated capture of events such as biometric measures (e.g. blood pressure, respiratory measures, ECG monitoring etc). - Instrumentation or electronic systems to capture, generate, manipulate or store data in an environment where analysis, tests, scans, imaging, evaluations, etc. are performed in support of clinical trials. - Electronic Health Records. Instruments and software used for the routine care of the patients and not supplied specifically for the purposes of a clinical trial, electronic medical files of the hospital or clinic and, laboratory instrumentation and diagnostic instrumentation in clinics are not the specific topic of this paper and whilst the principles set out here are also applicable in that context other issues also arise.
	6.1	General principles, paragraph 2: Section 5.5 of the Note for Guidance on Good Clinical Practice (CPMP/ICH/GCP/135/95)1 describes standards for the use of electronic trial data handling and/or remote electronic data systems. GCP requires that sponsors operating such systems validate the system, maintain SOPs for the use of the system, maintain an audit trail of data changes ensuring that there is no deletion of entered data, maintain a security system to protect against unauthorized access, maintain a list of the individuals authorized to make data changes, maintain adequate backup of the data, safeguard the blinding of the study and archiving of any source data (i.e. hard copy and electronic). If data are transformed during processing, it should always be possible to compare the original data and observations with the processed data. The sponsor should use an unambiguous subject identification code that allows identification of all the data reported for each subject. Sponsors are responsible for ensuring compliance with the requirements outlined above when tasks are subcontracted. There should be no loss of quality when an electronic system is used in place of a paper system.

Abbreviated Reference of Regulation/Guidance	Section	Description
FDA CFR 21 (11) Subpart B- Electronic Records	11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
	11.10 (b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
	11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.
	11.10 (d)	Limiting system access to authorized individuals.
	11.10 (e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
	11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
	11.10 (g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
	11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
	11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
	11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
	11.10 (k)	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
	11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.
FDA CFR 21 (11) Subpart C- Electronic	11.200 (a)	Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the

Abbreviated Reference of Regulation/Guidance	Section	Description
signatures		first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.
	11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.
FDA Guidance Part 11	Line 164 - 171	Under the narrow interpretation of the scope of part 11, with respect to records required to be maintained under predicate rules or submitted to FDA, when persons choose to use records in electronic format in place of paper format, part 11 would apply. On the other hand, when persons use computers to generate paper printouts of electronic records, and those paper records meet all the requirements of the applicable predicate rules and persons rely on the paper records to perform their regulated activities, FDA would generally not consider persons to be "using electronic records in lieu of paper records" under §§ 11.2(a) and 11.2(b). In these instances, the use of computer systems in the generation of paper records would not trigger part 11.
	173	2. Definition of Part 11 Records Under this narrow interpretation, FDA considers part 11 to be applicable to the following records or signatures in electronic format (part 11 records or signatures): - Records that are required to be maintained under predicate rule requirements and that are maintained in electronic format *in place of paper format*. On the other hand, records (and any associated signatures) that are not required to be retained under predicate rules, but that are nonetheless maintained in electronic format, are not part 11 records. We recommend that you determine, based on the predicate rules, whether specific records are part 11 records. We recommend that you document such decisions. - Records that are required to be maintained under predicate rules, that are maintained in electronic format *in addition to paper format,* and that *are relied on to perform regulated activities*. In some cases, actual business practices may dictate whether you are *using* electronic records instead of paper records under § 11.2(a). For example, if a record is required to be maintained under a predicate rule and you use a computer to generate a paper printout of the electronic records, but you nonetheless rely on the electronic record to perform regulated activities, the Agency may consider you to be *using* the electronic record instead of the paper record. That is, the Agency may take your business practices into account in determining whether part applies. Accordingly, we recommend that, for each record required to be maintained under predicate rules, you determine in advance whether you plan to rely on the electronic record or paper record to perform regulated activities. We recommend that you document this decision (e.g., in a Standard Operating Procedure (SOP), or specification document). -Records submitted to FDA, under predicate rules (even if such records are not specifically identified in Agency regulations) in electronic format (assuming the records have been identified in docket number 92S-0251 as the types of submissions the Agency accepts in electronic format). However, a record that is not itself submitted, but is used in

Abbreviated Reference of Regulation/Guidance	Section	Description
		generating a submission, is not a part 11 record unless it is otherwise required to be maintained under a predicate rule and it is maintained in electronic format. - Electronic signatures that are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules. Part 11 signatures include electronic signatures that are used, for example, to document the fact that certain events or actions occurred in accordance with the predicate rule (e.g. *approved*, *reviewed*, and *verified*).
FDA CSUCI	C	When original observations are entered directly into a computerized system, the electronic record is the source document. Under 21 CFR 312.62, 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain records required to be maintained under part 312, § 511.1(b), and part 812, for a period of time specified in these regulations. This requirement applies to the retention of the original source document, or a copy of the source document. When source data are transmitted from one system to another (e.g., from a personal data assistant to a sponsor's server), or entered directly into a remote computerized system (e.g., data are entered into a remote server via a computer terminal that is located at the clinical site), or an electrocardiogram at the clinical site is transmitted to the sponsor's computerized system, a copy of the data should be maintained at another location, typically at the clinical site but possibly at some other designated site. Copies should be made contemporaneously with data entry and should be preserved in an appropriate format, such as XML, PDF or paper formats.
	D1	Access must be limited to authorized individuals (21 CFR 11.10(d). This requirement can be accomplished by the following recommendations. We recommend that each user of the system have an individual account. The user should log into that account at the beginning of a data entry session, input information (including changes) on the electronic record, and log out at the completion of data entry session. The system should be designed to limit the number of log-in attempts and to record unauthorized access log-in attempts. We also recommend that passwords or other access keys be changed at established intervals commensurate with a documented risk assessment. When someone leaves a workstation, the person should log off the system. Alternatively, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, we recommend that a type of automatic protection be installed against unauthorized data entry (e.g., an automatic screen saver can prevent data entry until a password is entered).
	D2	It is important to keep track of all changes made to information in the electronic records that document activities related to the conduct of the trial (audit trails). The use of audit trails or other security measures helps to ensure that only authorized additions, deletions, or alterations of information in the electronic record have occurred and allows a means to reconstruct significant details about study conduct and source data collection necessary to verify the quality and integrity of data. Computer-generated, time-stamped audit trails or other security measures can also capture information related to the creation, modification, or deletion of electronic records. The need for audit trails should be determined based on a justified and documented risk assessment that takes into consideration circumstances surrounding system use, the likelihood that information might be compromised, and any system vulnerabilities. Should it be decided that audit trails or other appropriate security measures are needed to

Abbreviated Reference of Regulation/Guidance	Section	Description
		ensure electronic record integrity, personnel who create, modify, or delete electronic records should not be able to modify the documents or security measures used to track electronic record changes. Computer generated, time-stamped electronic audits trails are the preferred method for tracking changes to electronic source documentation. Audit trails or other security methods used to capture electronic record activities should describe when, by whom, and the reason changes were made to the electronic record. Original information should not be obscured though the use of audit trails or other security measures used to capture electronic record activities.
	D3	Controls should be established to ensure that the system's date and time are correct. The ability to change the date or time should be limited to authorized personnel, and such personnel should be notified if a system date or time discrepancy is detected. Any changes to date or time should always be documented. We do not expect documentation of time changes that systems make automatically to adjust to daylight savings time conventions. We recommend that dates and times include the year, month, day, hour, and minute and encourage synchronization of systems to the date and time provided by international standardsetting agencies (e.g., U.S. National Institute of Standards and Technology provides information about universal time, coordinated (UTC)). Computerized systems are likely to be used in multi-center clinical trials and may be located in different time zones. For systems that span different time zones, it is better to implement time stamps with a clear understanding of the time zone reference used. We recommend that system documentation explain time zone references as well as zone acronyms or other naming conventions
	E	We also recommend that controls be implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software.
	F2	The computerized system should be designed in such a way that retrieved data regarding each individual subject in a study is attributable to that subject.
	F4	When electronic formats are the only ones used to create and preserve electronic records, sufficient backup and recovery procedures should be designed to protect against data loss. Records should regularly be backed up in a procedure that would prevent a catastrophic loss and ensure the quality and integrity of the data. Records should be stored at a secure location specified in the SOP. Storage should typically be offsite or in a building separate from the original records. We recommend that you maintain backup and recovery logs to facilitate an assessment of the nature and scope of data loss resulting from a system failure.
	Appendix A	Standard operating procedures (SOPs) and documentation pertinent to the use of a computerized system should be made available for use by appropriate study personnel at the clinical site or remotely and for inspection by FDA. The SOPs should include, but are not limited to, the following processes. • System setup/installation (including the description and specific use of software, hardware, and physical environment and the relationship) • System operating manual • Validation and functionality testing • Data collection and handling (including data archiving, audit trails, and risk assessment)

Abbreviated Reference of Regulation/Guidance	Section	Description
		• System maintenance (including system decommissioning) • System security measures • Change control • Data backup, recovery, and contingency plans • Alternative recording methods (in the case of system unavailability) • Computer user training • Roles and responsibilities of sponsors, clinical sites and other parties with respect to the use of computerized systems in the clinical trials

2. Overview of regulatory conditions for acceptance of electronic source data

2.1 Introduction

The use of electronic source data in clinical trials, where the data are captured in an electronic form rather than on paper is becoming increasing prevalent. There are a wide variety of data that may be generated electronically in the conduct of a clinical trial, such as electronic Case Report Forms (eCRF), laboratory test results, ECGs, X-rays and patient diaries. However the current regulatory framework has not kept pace with this development and is still focussed on the use of paper source documents and paper-based processes rather than electronic source data and computer systems.

The Clinical Data Interchange Standards Consortium (CDISC) was set up to "develop and support global, platform-independent data standards that enable information system interoperability to improve medical research and related areas of healthcare". These data standards are applicable to both paper and electronic source data and the technology used to hold the data. They play an important role in meeting core regulatory requirements, even though they are not included in current regulations and guidance.

To further the use of eSource data in clinical trials, the eSource Data Interchange Group (eSID) was set up by CDISC with the specific objective "to produce a document that aligns multiple factors in the current regulatory environment, to encourage the use of eSource collection and industry data standards to facilitate clinical research for investigators, sponsors and other stakeholders". The publication "CDISC Standards and Electronic Source Data within Clinical Trials"[2] provides a set of 12 user requirements for source data. These requirements have been adopted by the European Medicines Agency (EMA) in their "Refection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials"[3] which provides the current opinion of the European GCP Inspectors Working group on the standards for the use of electronic data capture in clinical trials. This came into effect on 1 August 2010 and represents the most recent EMA thinking on this matter. This provides weight to use of these requirements in Europe, although there are other standards in operation.

In the USA, the FDA produced draft guidance for industry "Electronic source documentation in clinical investigations"[4] in December 2010 which focuses on the electronic Case Report Form (eCRF) as the vehicle used to collate all the data from different electronic and paper based systems. The guidance is intended to ensure reliability, quality, integrity and traceability of electronic source data and source records maintained at the site for FDA

[2] Electronic Source Data Interchange (eSDI) Group: Leveraging the CDISC Standards to Facilitate the use of Electronic Source Data within Clinical Trials, version 1.0, 20 November 2006

[3] GCP Inspectors Working Group: Reflection paper on the expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials, EMA/INS/GCP/454280/2010, 9 June 2010

[4] Guidance for Industry Electronic Source Documentation in Clinical Investigations December 2010, FDA

inspection. This document provides requirements for data entry, data review, data processing and transmission in the context of eCRFs.

As yet, there is no internationally agreed standard yet for eSource data requirements. Another aspect to consider is the increasing use of Electronic Health Records (EHRs) in institutions that conduct clinical trials. The primary use of an EHR is to record the medical history of the patient. The secondary uses include clinical research, identification of potential clinical trial subjects and data mining for trend analysis. EHR systems operate to various standards and degree of computer system validation and systems integration depending on the country and institution. This is insufficient to meet clinical research standards, which have to comply with specific regulatory requirements. Therefore source data held in EHRs may not be appropriate as source data for clinical studies for regulatory reasons. In this case the source data is entered into an Electronic Data Capture (EDC) system that requires a defined format of information using the EDC codes and requirements. The long term ideal is for single data capture so that source data in the EHR is interoperable with EDC systems.

The functionality of EHRs and associated systems for clinical research is being developed by the eClinical Forum and the PhRMAEDC/eSource Taskforce who have set up a global EHRCR Functional Profile Project. This taskforce has produced a set of minimum requirements for the use of EHR systems as the data source for clinical research[5]. A guide to support the configuration of EHR systems to meet clinical trial requirements is provided by the EHRCR (Electronic Health Records for Clinical Research) Working Group[6].

It is important that data protection requirements are met when personal data is processed from EHRs or other sources for clinical research. This is discussed in depth in the Report on regulatory requirements, confidentiality and data privacy issues. Part B: Confidentiality and data privacy framework.

2.2 Definitions

Source data:

All information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical trial necessary for the reconstruction and evaluation of the trial. Source data are contained in source documents (original records or certified copies).
Source: ICH GCP, Section 1.51

Source Documents:

Original documents, data, and records (e.g., hospital records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation checklists, pharmacy

[5] Requirements for EHR Systems Providing Source for Clinical Research: Electronic Health Records/Clinical Research EHRCR User Requirements Document (Release 2, January 2010)

[6] Practical Considerations for Clinical Trial Sites using Electronic Health Records (EHRs) In support of Clinical Research, Addressing Regulatory Considerations; Release 1.0 January 18, 2010 EHRCR (Electronic Health Records for Clinical Research) Working Group

dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate copies, microfiches, photographic negatives, microfilm or magnetic media, x-rays, subject files, and records kept at the pharmacy, at the laboratories and at medico-technical departments involved in the clinical trial).
Source: ICH GCP, Section 1.52

eSource:

Source data captured initially into a permanent electronic record.
Source: CDISC

Transcription:

Process of transforming dictated or otherwise documented information from one storage medium to another. NOTE: often refers explicitly to data that are manually transcribed from source docs or measuring devices to CRFs (i.e. Transcribed Data). (CDISC Clinical Research Glossary Version 8.0, DECEMBER 2009)[7].

2.3 Types of eSource data

The EMA Reflection paper defines the scope as “electronic systems, (including instruments, software and services) used in clinical trials in the creation/capture of electronic clinical data, such as:

- Electronic Case Report Forms (e-CRFs) e.g. laptop/desktop, mobile device based programs or web based tools, which may contain source data directly entered, transcribed data by re-keying from other sources, or both.
- Electronic patient data capture devices used to collect Patient Reported Outcome (PRO) data– e.g. mobile devices supplied to patients to record observations, rating scales, IMP use. This can be primary efficacy or supportive data.
- Instruments supplied to investigators for recording clinical data either by data entry or by automated capture of events such as biometric measures (e.g. blood pressure, respiratory measures, ECG monitoring etc).
- Instrumentation or electronic systems to capture, generate, manipulate or store data in an environment where analysis, tests, scans, imaging, evaluations, etc. are performed in support of clinical trials.
- Electronic Health Records. “

[7] CDISC (Clinical Data Interchange Standards Consortium) Clinical Research Glossary Version 8.0, DECEMBER 2009

2.4 Regulations and Guidance for eSource data

The EMA and FDA provide requirements for clinical trial records and the systems used to maintain them, although none relate specifically to eSource data.

Region	Reference/Title	Abbreviated reference
Inter-national	ICH Topic E6 (R1): Guideline for Good Clinical Practice Step 5	GCP
Europe	Directive 2001/20/EC: Implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use	EU 2001/20/EC
	Directive 2005/28/EC: principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products	EU 2005/28/EC
	Directive 95/46/EC: the protection of individuals with regard to the processing of personal data and on the free movement of such data	EU 95/46/EC
	EMEA Note for Guidance on Good Clinical Practice, CPMP/ICH/135/95, July 2002	CPMP/ICH/135/95
	GCP Inspectors Working Group: Reflection paper on expectations for electronic source documents used in clinical trials. 09 June 2010. Doc. Ref. EMA/INS?GCP?454280/2010	GCP Inspectors WG
	EudraLex - The Rules Governing Medicinal Products in the European Union. Volume 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use. Annex 11 - Computerized Systems'	Eudralex V4 Annex 11
USA	Electronic Records, Electronic Signatures Final Rule (21 CFR Part 11, 20-Mar-1997)	FDA CFR 21 (11)
	FDA Guidance for Industry. Part 11, Electronic Records; Electronic Signatures – Scope and Application (August 2003)	FDA Guidance Part 11
	FDA Guidance for Industry. Computerized Systems Used in Clinical Investigations (May 2007)	FDA CSUCI
	Good Clinical Data Management Practice, Version 4, Society for Clinical Data Management, October 2005.	
	FDA Draft Guidance for Industry. Electronic Source Documentation in Clinical Investigations, Dec 2010	

Details of these documents are provided in Table 6

The specific requirements to comply with Good Clinical Practice (ICH E6 (R1) and CPMP/ICH/135/95) are provided in sections 2.10, 4.9,3 and 5.5.3 – 5.5.5 [Table 6]. These relate to clinical trial information, (paper) CRF and electronic trial data handling.

2.5 Regulatory conditions for acceptance of eSource data

Electronic data capture is currently used in clinical trials and has to meet the regulations and guidance documents outlined in the previous section. However most of these documents do not specifically address eSource data requirements or the use of EHRs. The recently published EMA Reflection paper and draft FDA guidance on eSource documentation are beginning to address this.

Standards for eSource data are being developed, but are driven by different groups. In clinical research CDISC provide the direction. In the healthcare sector, where EHRs are becoming more widely used, there are two organisations providing direction for the

certification of EHR systems: Health Level 7 Inc., known as HL7 (an American standards development organization) and EuroRec (European Quality Labelling and Certification of Electronic Health Record), the European Union EHR certification committee. However this certification does not mean that the EHR system fully meets all the regulatory requirements of clinical research. HL7 and EuroRec agreed on the setting up of the Electronic Health Record for Clinical research (EHRCR) Project to determine how to fully integrate healthcare and research systems. As part of this the EHRCR Functional profile was developed, which provides the requirements for an EHR system to meet clinical research regulations and guidance.

The following sections show the user requirements developed by CDISC and by the global EHRCR Functional Profile Project.

There is a great deal of activity in the field of eSource data. The work on its acceptance in clinical research encompasses the desire for single data capture and the interoperability of EHR with other systems such as EDC. However different groups are working in this field and the standards being generated need to be harmonised. Integrated IT solutions are also required to support clinical data collection, such as Clinical Trial Data Management Systems (CTDMS).

Compliance with the regulations and guidance for clinical research, combined with the CDISC user requirements for eSource data are necessary for acceptance of eSource data at present. eSource data taken directly from EHR represents a greater challenge, since the EHR and system must meet clinical research standards.

2.6 CDISC 12 User Requirements and practical considerations

The CDISC eSDI Working Group identified 12 user requirements that an eSource system must fulfil, based on FDA guidance and ICH GCP. The practical consideration of each requirement is taken for the EMA Reflection paper. These user requirements provide the standards for eSource data and systems in the absence of specific regulations or guidance. Since they are based primarily on ICH GCP they should be acceptable internationally. This is of particular importance for clinical trials, which can be conducted globally.

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
Creation and modification of systems				
1	An instrument used to capture source data shall ensure that the data is captured as specified within the protocol.	An instrument used to generate, capture, transfer, manipulate or store data (e.g. Case Report Form (CRF), patient diary, site-designed worksheet) should be an accurate representation of the protocol ensuring that the data as specified within the protocol can be captured correctly and that the investigator or subject response is not biased by default values present within the instrument. Where applicable, the availability of an optional free text field for investigators to record additional information is encouraged. The instrument should be created in a controlled manner to ensure that it conforms to the protocol and is validated. In addition, appropriate change control as part of ongoing validation is needed, in cases where protocol amendments require changes to the instrument. Records of system validation including requirements, design, installation, access and security, testing (e.g. user acceptance testing, installation, operational and performance testing), training and controlled release for use should be maintained.	2.6 and 6.4.9	The sponsor and vendor designed the eSource application and the configuration of the diary within it to match the protocol specifications. Testing was performed to insure the functionality matched the protocol. **Investigator responsibility**: Notify the sponsor of any deviations in the eSource design from protocol requirements.
Creation, modification and transfer of data				
2	Source data shall be Accurate, Legible, Contemporaneous, Original, Attributable, Complete and Consistent.	Accurate: The use of such instruments/systems should ensure that the data are at least as accurate as those recorded by paper means. The validity of the data capture process is fundamental to ensuring that high-quality data are	1.5.1, 1.5.2, 4.9.1 and 6.4.9	The eSource system is programmed and validated to increase accuracy, legibility, completeness, and timeliness of data collection. Attributability needs

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
		produced as part of a trial. The process needs to ensure that all data required are captured and that data are captured in a consistent manner. The coding process which consists in matching text or data collected on the CRF to terms in a standard dictionary, thesaurus or tables (e.g. units, scales, etc.) should be controlled. The process of data transfer between systems should be validated. Legible: Readable at the input and output stage in a form meaningful to an independent reviewer i.e. a human being should be able to read it, not encrypted, coded or in programmed language. Contemporaneous: The recording of a clinical observation is made at the same time as when the observation occurred. If this is not possible the chronology of events should be recorded. An acceptable amount of delay should be defined and justified prior to trial recruitment. Original: This must be the first record made by the appropriate person e.g. ePRO record produced by the subject and not the investigator or the first acceptable result generated in an environment where analysis, tests, scans, imaging, evaluations, etc. are performed in support of clinical trials. Attributable: The person undertaking the action should be recorded by the system. Unique user identification is necessary (login, username, password, PIN etc.), and this needs to account for the fact that many trials are conducted at multiple locations, and permit entries to be consolidated into a central database. As with hard copy paper data, it is important that electronic data are time/date stamped when the data are created/generated. Reasonable controls should be established to help assure that user identification truly represents that individual (i.e. there is no identity theft). Completeness and consistency: can be assisted by the use of features such as drop-down lists, online edits, check boxes		to be assured by the system (login, username, password etc.). **Investigator responsibility**: 1) Monitor compliance of patients in completing eSource as scheduled. Monitor completeness of data in a timely fashion. 2) Maintain and oversee security of pass-codes for devices and web reports for their studies. 3) Verify accuracy of date and time stamps applied by the system

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
		and branching of questions or data entry fields based on entries. The individual (investigator site staff, study subjects, caregivers or others) capturing the data need to have documented training in the correct use of the instrument and the electronic data capture document. In addition, when considering data from an environment where analysis, tests, scans, imaging, evaluations, etc. are performed in support of clinical trials, it should be possible to fully reconstruct the activities performed. Electronic checks do not automatically remove the need for review of data by the investigator or other experts, or by the monitor / data manager depending on the nature, purpose and importance of the items involved. Data should be traceable and an unambiguous subject identification code should be used to allow identification of all data reported for each subject. A procedure should be in place to address the situation when a study subject or other operator capturing data, realises that he/she has made a mistake and wants to correct the recorded data. It is important that original electronic entries are visible or accessible (e.g. in the audit trail) to ensure the changes are traceable. Any transfer from paper to electronic CRF should be subject to quality control and the level of control should be justified.		
3	An audit trail shall be maintained as part of the source documents for the original creation and subsequent modification of all source data	The maintenance of an audit trail is essential to ensure that changes to the data are traceable. Secure, computer-generated, time-stamped audit trails (or alternative methods that fulfil the audit trail requirements) should be used to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Such audit trail documentation should be retained as long as the subject electronic records. Audit trails need to be readable and changes to audit trail data should be prevented by the system. The responsible investigators, sponsors and	4.93 and 5.5.4	The eSource system was designed with a full audit trail. **Investigator responsibility**: 1) Any data changes must be made according to established SOP(s) using the eSource system software. 2) Review the audit trail.

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
		inspectors should be able to review the audit trail. The audit trail will record changes made as a result of data queries or a clarification process. The clarification process for data entered by trial subjects should be documented and it should be clearly stated where changes to data entered by subjects will not be made.		
4	The location of source documents and the associated source data shall be clearly identified at all points within the capture process.	The protocol should identify any data to be recorded directly into the CRFs that is considered to be source data. A detailed diagram and description of the transmission of electronic data should be provided in the protocol. The source data and their respective capture methods should be clearly defined prior to trial recruitment (i.e. in the protocol or study specific source data agreement). The sponsor should describe which data will be transferred, the origin and destination of the data, the parties with access to the transferred data, the timing of the transfer and any actions that may be triggered by real-time review of those data. There should only be one source defined at any time for any data element. Considering the electronic source data environment it is accepted that the earliest practically retainable record should be considered as the location of the source data and therefore the source document. In this case the process should be clearly documented and the protocol should state which data recorded on the instrument will be used as the official source data. There is a need to capture the logical location (e.g. a folder) of the source data. When data are created, copied or transferred the final location and identification (source, copy or back-up) should be documented.	6.4.9	**Investigator responsibility**: 1) The investigator should be aware of where the source data are being held during the life of the trial and during the period of source data retention.
Control				
5	The investigator shall maintain the original source document or a	The fundamentals of clinical research include that patient rights, safety and well-being are the most important	2.11, 5.15.1	The source data are stored on the device and then certified copy is

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
	certified copy.	considerations and the integrity of the reported data must be confirmable. To this end all data generated in a clinical trial relevant to patient care must be made available to the investigator at all times during and after the trial and all data held by the sponsor that has been generated in a clinical trial should be verifiable to a copy not held (or that has been held) by the sponsor. The requirements above are not met if data are captured in an electronic system and the data are stored on a central server under the sole control of the sponsor. This is because the investigator does not hold an independent copy of the data and therefore the sponsor has exclusive control of the data. In order to meet the requirements a contemporaneous certified copy of the data should be retained at the investigator site in addition to the record maintained on a central server. The requirement 7 above is not met if data are captured in an electronic system and the data are stored on a central server not under the control of the sponsor, but eventually are transferred to the sponsor. This is because the sponsor has exclusive control of the data. In order to meet the requirements a certified copy of the data should be created before the transfer to the sponsor and retained at the investigator site. The method of transfer should be validated The sponsor of a study remains ultimately responsible for the quality of the study data and for ensuring that procedures, system controls and contracts/agreements are in place to protect this quality. The investigator should ensure the accuracy, completeness, legibility and timeliness of the data reported to the sponsor in the CRFs and in all required reports (ICH GCP 4.9.1). Part of the processes in place to achieve this could be the use of service providers that furnish the hardware and may manage the software and data capture receipt and storage. A service provider collecting or storing data should be a separate legal entity from the		transferred to server. **Investigator responsibility**: 1) The investigator must understand how to access the certified copy on the server. 2) The investigator must approve any changes to source data. 3) The investigator must store and maintain the final archival study file with the certified copy of their site's source data.
6	Source data shall only be modified with the knowledge or approval of the investigator.		4.9.3, 4.9.4 and chapter 8	Data management SOPs require investigator approval of any data changes. A full audit trail is available to document changes. **Investigator responsibility**: 1) The investigator must approve any changes to source data. 2) Review the audit trail.
7	The sponsor shall not have exclusive control of a source document.		8.3.13	eSource vendor holds multiple copies of the source data. Any data changes must be approved by the investigator. **Investigator responsibility**: 1) The investigator must approve any changes to the source data.

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
		sponsor and from the investigator. A detailed contract should be in place defining the duties of the service provider, enabling the sponsor and/or investigator to transfer some of their tasks, but to retain control of their responsibilities. The contracts/agreements with the sponsor and with the investigator will need to make clear the role of the service provider and to what extent this relates to the specific responsibilities of the investigator and those of the sponsor. The method by which it is ensured that the investigator is informed about and/or approves of modifications to the data should be clearly established, and this control by the investigator should be demonstrable. Any changes to the data should be captured by the audit trail (see requirement 3). This includes any modifications arising from data query or clarification processes. The investigator should have access to review the data on an ongoing basis.		
8	Source documents shall be protected against unauthorized access.	Source documents need to be protected in order to maintain subject confidentiality. Changes or deletion by unauthorised individuals, either accidental or deliberate, should be prevented. Authority checks should be used, as these could ensure that only authorised individuals have access to the system, or the ability to enter or make changes to data. Records of authorisation of access to the systems, with the respective levels of access clearly documented (e.g. individual user accounts) should be maintained. Audit trails should record changes to user access rights. There should be documented training on the importance of security including the need to protect and not share passwords as well as enforcement of security systems and processes. The system users should confirm that he/she accepts responsibility for data entered using their password. Security systems should prevent unauthorised access to the computer system and to the data in the electronic record. Procedures should be in place to avoid/prevent unauthorised access	2.11, 5.15.1	The eSource system has pass-code security controls to protect against unauthorized access. **Investigator responsibility**: 1) Maintain and oversee security of pass-codes for devices and web reports. 2) The investigator must protect the final archival media in their possession from unauthorized access.

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
		when a workstation is vacated. There should be timely removal of access no longer required, or no longer permitted.		
Copying				
9	The source document shall allow for accurate copies to be made.	It is a fundamental requirement that a source document and data can be copied and that there is a practical method of copying that is complete and accurate, including relevant metadata. When required, it should be possible to print the source document/data for review, audit or inspection purposes.	1.51	Procedures for producing certified copies have been validated. **Investigator responsibility**: 1) Ensure the investigator knows how to generate copies
10	When source data are copied, the process used shall ensure that the copy is an exact copy preserving all of the data and metadata of the original.	Accurate and complete copies for certification should include the meaning of the data (e.g. date formats, context, layout, electronic signature and authorisations), as well as the full audit trail. The investigator site should have the ability of reviewing the data and generate copies. Where certified copies are made the process for certification should be described, including the process for ensuring that the copy is complete and accurate and for identifying the certifying party and their authority for making that copy. The process of making a "certified copy" needs to be validated.		**Investigator responsibility**: 1) In the electronic world the investigator should be aware that the system in use has been validated for the purposes of clinical research..
Storage				
11	The storage of source documents shall provide for their ready retrieval.	Source documents and data should always be available when needed to authorised individuals to meet their regulatory obligations. Whilst a trial is active and after its conclusion, existing source data should be readily available to the investigator and others such as monitors, auditors and inspectors. Direct access to the system should be provided by the sponsor and/or investigator to monitors, auditors and inspectors.	2.11, 5.15.1	The source data are stored on a centralized server with retrieval access provided through the web reports. **Investigator responsibility**: The investigator must understand how to access the source data.
12	Source documents and data shall be protected from destruction.	Source data should be protected from destruction, either accidental or deliberate. Regular backups should be made. Suitable archiving systems should be in place to safeguard the data integrity for the periods established by the regulatory requirements including those in any of the regions where the	4.9.3, 4.9.4 and chapter 8	The eSource system keeps a duplicate certified copy of the source data in a separate location to protect physical destruction. Backup and security systems are also in place.

No.	User Requirement	Practical consideration of user requirement	ICH GCP Reference	Met By
		data may be used for regulatory submissions, and not just those of the country where the data are generated. Checks of accessibility to archived data, irrespective of format, including relevant metadata, should be undertaken to confirm that the data are enduring, continue to be available, readable and understandable by a human being.		**Investigator responsibility**: 1) The investigator must protect the final archival media from destruction for the time period specified by the sponsor and **existing** regulations.

2.7 EHRCR User requirements

The Electronic Health Record for Clinical Research (EHRCR) User requirements, which relate specifically to computerised EHRs used in Clinical Research provide the core requirements for EHR systems to meet current regulations and guidance for clinical research and are the basis for the EHRCR Functional Profiles, in both HL7 and EuroRec formats.
The criteria for the core level of the EHRCR Functional Profile

- Research Identifiers
    - The system must have the ability to capture, store, and associate research identifiers with patients who are enrolled in clinical trials. These identifiers include subject number, protocol identifier, investigator identifier, and site identifier. These clinical-research identifiers should be included on all subject information output.
- Additional data elements
    - In addition to structured domain data already collected in an EHR system, a minimum set of additional domain data, as modelled by CDISC CDASH, are included for the following domains: Demographic, Medical History, Medication, Adverse Event, Physical Exam, Vital Signs

In order to meet clinical research regulations, the criteria in the following categories were added:

- Added privacy features:
    - Additional features for de-identifying research-bound data such that privacy regulations are met (e.g. ability to mask patient identifiers in data that will be shared with research)
- Added security features:
    - Additional security requirements (e.g. limiting number of login attempts, record failed log-in attempts, enforce periodic password change, automatic “screen lock” after a period of inactivity, limiting access to audit trail and clock, restrict data viewing)
- Added audit trail features:
    - Additional Audit trail capabilities (e.g. a method to enable local time to be derived, feature to maintain a synchronization of audit trail to master clock, ability to indicate reason for modifications, and maintenance of audit trail record after its associated patient record has been deleted)
- Produce a research-appropriate copy of data:
    - Produce human-readable copy of research-bound data and associated audit trail (e.g. in PDF or XML format)

The HL7 Functional Profile was approved as an American National Standards Institute (ANSI) standard in July 2010. The European equivalent, a CEN standard has not been issued yet. The intention of having accepted standards is to enable certification of the EHR systems.

2.8 Investigator and sponsor responsibilities for EHRs

The investigator, staff and associated laboratories generate electronic data, such as eCRF or patient diaries, using a variety of software and hardware, possibly using their own. To meet GCP requirements the responsibilities of the investigator and the sponsor should be clearly defined from the initial data capture through to handling of the data in the clinical trial database. The sponsor (or contracted service provider) supplies and/or operates electronic recording systems and manages the records generated by them. The reliability of the data needs to be demonstrated which includes validation of the electronic system. The sponsor must assess whether the systems used by the investigator meet GCP including the 12 CDISC user requirements. The assessment should include the potential harm to patients and the data integrity of the trial. If the systems do not meet GCP requirements mitigating actions should be taken prior to site initiation.

3. References

Reference/Title	Web address
ICH Topic E6 (R1): Guideline for Good Clinical Practice Step 5 CPMP/ICH/135/95	http://www.ich.org/products/guidelines/efficacy/article/efficacy-guidelines.html
ISO 27001: Information Security Management – Specification with Guidance for Use	Not available for download
Directive 2001/20/EC: Implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use	http://ec.europa.eu/health/documents/eudralex/vol-1/index_en.htm
Directive 2005/28/EC: principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products	http://ec.europa.eu/health/documents/eudralex/vol-1/index_en.htm
EMEA Note for Guidance on Good Clinical Practice, CPMP/ICH/135/95, July 2002	http://www.ema.europa.eu/pdfs/human/ich/013595en.pdf
GCP Inspectors Working Group: Reflection paper on expectations for electronic source documents used in clinical trials. Effective date: 1 August 2010. Ref. EMA/INS/GCP/454280/2010	http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/document_listing/document_listing_000136.jsp&murl=menus/regulations/regulations.jsp&mid=WC0b01ac05800296c4
EudraLex - The Rules Governing Medicinal Products in the European Union. Volume 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use. Annex 11 - Computerized Systems'	http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm
Electronic Records, Electronic Signatures Final	http://www.accessdata.fda.gov/scripts/cdrh/cfdoc

Reference/Title	Web address
Rule (21 CFR Part 11, 20-Mar-1997)	s/cfcfr/CFRSearch.cfm
FDA Guidance for Industry. Part 11, Electronic Records; Electronic Signatures – Scope and Application (August 2003)	http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM072322.pdf
Guidance for Industry: E6 Good Clinical Practice: Consolidated Guidance (ICH April 1996)	http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm065004.htm
FDA Guidance for Industry. Computerized Systems Used in Clinical Investigations (May 2007)	http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM070266.pdf
Good Clinical Data Management Practice, Version 4, Society for Clinical Data Management, October 2005.	http://www.scdm.org/gcdmp/
Implementation of Good Clinical Practice Software, Lauritsen J M, University of Southern Denmark (02/2007, Draft)	
German Coordinating Centres for Clinical Trials networks Policy Document (October 23rd 2001, updated December 20th 2007)	
Data and Information Management Systems Project - System Standards - UKCRC / NIHR (2009)	
IT-Grundschutz Methodology, Bundesamt für Sicherheit in der Informationstechnik (BSI).	
Directive 95/46/EC: the protection of individuals with regard to the processing of personal data and on the free movement of such data	http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
Méthodologie de Référence – MR001 (Benchmark standards for personal data processing in GCP-clinical trials). Published by the French Data Protection Authority - Commission national de l'informatique et des libertés (CNIL)	http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article//une-procedure-simplifiee-de-declaration-pour-les-recherches-biomedicales/ http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/sante/chapIX.pdf
Guidelines for Data Processing within the Framework of Clinical Drug Trials - 24 July 2008 Published by the Italian Data Protection Authority "GARANTE"	http://www.garanteprivacy.it/garante/doc.jsp?ID=1533155 http://www.garanteprivacy.it/garante/doc.jsp?ID=1671330 (English version)
Standards for clinical trial personal data processing	http://www.medicamentos-innovadores.org/documentos/C%20Tipo(10-11-09)(publicaciónAEPD).pdf
Data Protection Guidelines on Research in the Health Sector November 2007	http://www.dataprotection.ie/documents/guidance/Health_research.pdf
The personal data act, clinical trials and data privacy. Rules for treatment of personal data in	http://www.ncbi.nlm.nih.gov/pubmed/12756831

Reference/Title	Web address
clinical trials and scientific research projects.	
Use and Disclosure of Health Data. May 2002. Guidance on the Application of the Data Protection Act 1998	http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/health_data_-_use_and_disclosure001.pdf
The eClinical Forum and PhRMA EDC/eSource Taskforce (2006): The future vision of electronic health records as eSource for clinical research. Version 1.0, 14 September 2006	http://www.eclinicalforum.org/Knowledge/tabid/54/Default.aspx
Clinical Data Interchange Standards Consortium, Electronic Source Data Interchange (eSDI) Group (): Leveraging the CDISC Standards to Facilitate the use of Electronic Source Data within Clinical Trials. Version 1.0, 20 November 2006	(http://www.cdisc.org/stuff/contentmgr/files/0/2f6eca8f0df7caac5bbd4fadfd76d575/miscdocs/esdi.pdf)
Pharmaceutical Inspection Convention, PIC/S Guidance: Good practices for computerized systems in regulated “GXP” environments, 25 September 2007	(http://www.picscheme.org/publication.php?id=8)
Electronic Health Records for Clinical Research (EHRCR) Working Group (2010): Practical considerations for clinical trial sites using electronic health records (EHRs) in support of clinical research. Adressing regulatory considerations. Release 1.0, January 18, 2010	http://www.eclinicalforum.org/LinkClick.aspx?fileticket=18S2CJFc-WE%3d&tabid=344&language=en-GB
EHRCR Functional Profile Working Group, eClinicalForum and PhRMA EDC/eSource Task Force: EHRCR User requirements Document, January 2010	http://www.eclinicalforum.org/LinkClick.aspx?fileticket=MIgYEPcWCtg%3d&tabid=344&language=en-GB
EHRCR Working Group: Electronic Health Records/Clinical Research: EuroRec Electronic Health Records for Clinical Research Functional Profile, Version 1.0 January 2010	http://www.eclinicalforum.org/Knowledge/tabid/54/Default.aspx
Clinical Data Acquisition: Standards Harmonization (CDASH), CDASH_STD-1.0, 01/OCT/2008	http://www.cdisc.org/stuff/contentmgr/files/0/9b32bc345908ac4c31ce72b529a3d995/misc/cdash_std_1_0_2008_10_01.pdf
European Clinical Research Infrastructures Network (ECRIN) and Biotherapy Facilities: Preparation Phase for the Infrastructure: Standard requirements for GCP-compliant data management in multinational clinical trials; Ref. ECRIN-PPI No. 211738	Published as free article: Ohmann C et al.: Standard requirements for GCP-compliant data management in multinational clinical trials. Trials 2011; 12: 85 (see additional file)