ISO/IEC JTC 1/SC 32 N 2327

Date: 2013-03-09

REPLACES: –

ISO/IEC JTC 1/SC 32

Data Management and Interchange

Secretariat: United States of America (ANSI)
Administered by Farance Inc. on behalf of ANSI

DOCUMENT TYPE	Outgoing Liaison Statement
TITLE	Liaison ballot comments to ISO TC 215 regarding ISO DTS 14441 from JTC1 SC32 Data Management and Interchange
SOURCE	SC 32 Secretariat
PROJECT NUMBER	1.32.31.01.08.00
STATUS	SC32 liaison ballot comments on ISO TS 14441 Health Informatics - Security and privacy requirements
REFERENCES	
ACTION ID.	FYI
REQUESTED ACTION	
DUE DATE	--
Number of Pages	41
LANGUAGE USED	English
DISTRIBUTION	P & L Members SC Chair WG Conveners and Secretaries

Dr. Timothy Schoechle, Secretary, ISO/IEC JTC 1/SC 32
Farance Inc *, 3066 Sixth Street, Boulder, CO, United States of America
Telephone: +1 303-443-5490; E-mail: Timothy@Schoechle.org
available from the JTC 1/SC 32 WebSite http://www.jtc1sc32.org/
*Farance Inc. administers the ISO/IEC JTC 1/SC 32 Secretariat on behalf of ANSI

DOCUMENT TYPE	Outgoing liaison ballot comments
TITLE	JTC1/SC32 to ISO 215 Liaison ballot comments on document TC215 N1138 *ISO/TS 14441 Health Informatics – Security and privacy requirements of HER systems for use in conformity assessment*
SOURCE	JTC1/SC32 liaison to ISO TC215
PROJECT NUMBER	
STATUS	
REFERENCES	
ACTION ID	For consideration by TC 211
REQUESTED ACTION	To be addressed and resolved as part of ballot comment resolution process for ISO TS 14441
DUE DATE	
Number of pages	36
LANGUAGE USED	English
DISTRIBUTION	ISO TC215 members, JTC1/SC32 members
Notes	1. The ballot comments made in this document are based on ISO/IEC IS 15944-8:2012 *Information technology – Business Operational View – Part 8: Identification of privacy protection requirements as external constraints on business transaction.* This IS was developed by *ISO/IEC JTC1/SC32 "Data management and interchange".* JTC1/SC32 focuses on application sector independent, i.e., generic (or horizontal) standardization requirements including those of an electronic data interchange (EDI) nature. 2. The ISO/IEC 15944-8 "privacy protection" standard document has already been communicated to ISO TC215 via an earlier liaison as document JTC1/SC32 N2295. Note that ISO/IEC 15944-8 is an "ISO freely available standard" {see further www.iso.org/PubliclyAvailableStandards }. One notes here that all the Parts of the multipart ISO/IEC 15944 eBusiness series of standards are also publicly available standards as is the ISO/IEC 14662 *Open-edi Reference Model* (which is also a publicly available standard). 3. A primary reason that ISO made the ISO/IEC 15944 series of standards, freely/publicly available, is that they are intended to provide the basis for use by other standards developers in that or related fields. In the field of "privacy protection", ISO/IEC 15944-8 fulfills this role. In this context, it is noted that the following standard developed by ISO/IEC JTC1/SC36 eLearning has made extensive use of the "generic" ISO/IEC 15944-8 standard in its development of its ISO/IEC 29187-1:2013 *Information technology – Identification of privacy protection requirement pertaining to learning, education and training (LET) – Part 1; Framework and reference model".* As such JTC1/SC36 benefited from using the "generic" privacy protection stand of JTC1/SC32 and adapted it to the specific needs of the learning, education and training (LET) sector.

JTC1/SC32 Liaison Comments on the ISO TC215 ballot document N1138 for " ***ISO/TS 14441 – Health informatics – Security and privacy requirements of HER systems for use in conformity assessment*****"**

Date: 2013-03-09	Document: **ISO/TS 14441**

1	2	(3)	4	5	(6)	(7)
MB[1]	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/Note** (e.g. Table 1)	**Type of com-ment**[2]	**Comment (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations** on each comment submitted
SC 32-00	All	All	Ge	1. ISO/IEC JTC1/SC32 liaison to ISO TC 215 welcomes this opportunity to comment on the ISO/TS 14441 and trusts that these comments will be helpful to TC215 in the completion of the development of this standard project. The ISO/IEC JTC1/SC32 liaison to ISO TC215 is also the Project Co-Editor for the ISO/IEC 15944-8:2012 ".privacy protection.." standard whose complete title is *"Information technology – Business Operational View – Part 8: Identification of privacy protection requirements as external constraints on business transactions*". 2. It is noted that ISO/IEC 15944-8 is part of a series of generic information technology eBusiness standard, and as such is intended to serve not only general users but in particular standards developers in specific domain field	1. Should ISO TC215 Project Editor(s) for ISO/TS 14441 wish to communicate directly with the JTC1/SC32 liaison to TC215 in his role as Project Co-Editor for ISO/IEC 15944-8, this can be done directly by contacting Dr. Jake V. Knoppers at < mpereira@istar.ca > [or as back-up e-mail at < jk0@istar.ca > (or Steve Matthews at < stevem2@compuserve.com > . 2. Ballot comments made below are intended to share with TC 215, the results of over 15 years of EDI and eBusiness standards development and use of JTC1/SC32 "Data management and interchange" in general and "privacy	

[1] For these ballot comments, "SC32" is used as the reference for these ballot comments by JTC1/SC32 Liaison to ISO TC215

				including that of “eHealth”. As such the ISO/IEC 15944 eBusiness series of standards paid particular care in the development of key concepts and their definitions (and related constructs) being generic in nature addressing cross-sectoral issues while also serving as a bridge to relevant legal constructs and requirements. [Note: “privacy protection” is a legal construct and requirement, not to be confused with “confidentiality”]. 3. In this context, one should also note that, a) “business transaction” is a type of commitment exchange, pertaining to the making and executing of commitments among autonomous parties. The approach taken in the multipart ISO/IEC 15944 series of standards is that e-business includes and can be conducted on both a for-profit and not-for-profit basis. The latter is the case in many countries in the provision of health care. b) “privacy protection” draws its definition from the fact that it is a legally introduced and enforced set of requirements as a set of rights of an individual and set of concomitant obligations of organizations which collect, manage, interchange and safeguard personal Information.	protection” in particular in support of further development of TS 14441. 3. For ISO definitions of these concepts see further in ISO/IEC 15944-8 a) for “**business transaction**” see Clause 3.11 b) for ”**privacy protection**”, see Clause 3.108	
SC	All	All	Ge	JTC1/SC32 in its development of the multipart	1. JTC1/SC32 assumes that the	

32-01				ISO/IEC 15944 eBusiness standards maximize use and re-use of existing ISO standards where and wherever applicable. Here the development of its ISO/IEC 15944-8 "… privacy protection requirements .." standard has cites and uses as Normative References, twenty-four (24) other international standards, and six (6) references specifications (which are of the nature of international legal requirements0. In this context, ISO/IEC 15944-8 also utilized the following ISO TC215 standards which contain key concepts and their definitions which where incorporated as is or as adapted, namely, ISO 22857 -2004 (E) *Health informatics Guidelines on data protection to facilitate trans-border flows of personal health information*; and, ISO/TS 25237:2008 *Health informatics - Pseudonymization*	development of ISO/TS 14441 with respect to privacy protection requirements will also ensure that a) this standard development work is harmonized with the privacy protection requirements of its TC 215 existing ISO 22857 and ISO/TS 25237 standards; and, b) incorporates the same in its Clause 2 "Normative References" (or Bibliography). 2. JTC1/32 requests ISO TC215 in its further development of ISO/TS 14441 to take into consideration and maximize use of ISO/IEC 15944-8 as a Normative Reference, and in particular its Clause 3 Definitions. (as and where applicable). 3. JTC1/SC32 assumes that EHR systems need/will engage in electronic data interchange (EDI) with IT systems of other organizations and public administrations. This is because the Clause 1 Scope statement contains the following text " ..*are also interoperable with EHRs"*. Therefore, it is most likely that the existing ISO/IEC 14662 and ISO/IEC 15944-8 standards need to be taken into account and ISO/IEC 15944-8 serve as a Normative Reference in Clause 2 for this further development of	

					this ISO/TS 14441 standard. {See also below SC32 liaison comments 6 ->9 on Clause 1 Scope}	
SC 32-02	All	All	All	The JTC1/SC32 liaison comments are directed primarily at text in Clause 1 – Scope, and Clause 3 Terms and Definitions. Time and resource constraints of JTC1/SC32 liaison to TC 215 prevent making a much more complete and thorough set of ballot comments. However, one welcomes a more intensive interchange between ISO/IEC JTC1/SC32 and ISO TC 215 liaisons/experts in the further development and completion of the ISO/TS 14441 standard based on resolution of the ballot comments of JTC1/SC32.	A possible useful follow-up here would be for TC215 to establish support direct communication and interworking between its Project Editor(s) for the further development of ISO/TS 14441 and the Project Co-Editors for the existing ISO/IEC 15944-8 standard.	
SC 32-03	All	All	All	1. Need to avoid confusion on the use of the word “person” throughout the document, i.e., when is it intended to refer to persons in general and when to individuals only or when to organizations and public administrations only? {See Clause 0.2, in ISO/IEC 15944-8.} 2. Here JTC1/SC32 in its development of its multipart ISO/IEC 15944 eBusiness	JTC1/SC32 requests TC215 to consider replacing “person” and “entity” with the existing ISO concepts and definitions of **> Person** [for text see Clause 3. in ISO/IEC 15944-8] **> individual** [for text see Clause 3. in ISO/IEC	

				standards took not of and supported the international legal and pragmatic fact that there was a major confusion in the English language in its use of the character string “person”. It was not clear whether the use of this character string of “person”, pertained solely to an “individual. 3. Here JTC1/SC32 in its development of its multipart ISO/IEC 15944 eBusiness standards, took not of and supported the international legal and pragmatic fact that there was a major confusion in the English language in its use of the character string “person”. It was not clear whether the use of this character string of “person” pertained solely to an “individual human being” or also included an “artificial or legal person”. 4. JTC1/SC32 successfully addressed this major issue by introducing the concept of “**Person**” in ISO standards (with a capital “P”, with a definition for this new concept which serves as an umbrella (or super-type) concept to cover situations and application of a constraint on both natural persons and legal persons. This approach for “Person” then allows and facilitates the use of three sub-types of Person, namely, - **individual**, i.e., a natural person acting and making decisions on its behalf only, having privacy protection right, etc.;	15944-8] **> organization** [for text see Clause 3. in ISO/IEC 15944-8] **> public administration** [for text see Clause 3. in ISO/IEC 15944-8] as and where applicable. These Clause 3 Definitions also provide the references to the existing ISO standards whose concepts and their definitions were used to develop ISO/IEC 15944-8 and are relevant to privacy protection requirements... -	

				- **organization**, i.e., any kind of artificial or legal person, for-profit, not-for-profit, etc.; and, - **public administration**, i.e., **Person** which is an **organization** and has the added attribute of acting on behalf of a **regulator**		
SC 32-04	All	All	te/ed	It is a not uncommon occurrence that some use confidentiality and privacy as 'synonyms. They are not. "confidentiality" is something that is agreed to among participating parties (often as part of a contractual obligation. "privacy protection, on the other hand, is a right of an individual to source of which is public policy (in the form of laws & regulations of applicable jurisdictional domain(s), international treaties, "directives", etc. Need assurance that privacy protection requirements are part of public policy requirements which pertain only to an "individual" (as a natural person, human being) and that organizations or public administrations do not have "privacy protection rights", i.e., only obligations to support and implement the same.	It is recommended that at the outset, either in the Clause 0 Introduction or early in Clause 5 plus to a) state that privacy protection is a right of an individual as stated in applicable public policy; and, b) that "confidentiality" should not be viewed as a synonym of privacy (and should be viewed as just one of several privacy requirements).	

SC 32-05	All	All	te	ISO/IEC JTC1/ SC32 liaisons to ISO TC215 have prepared a number of technical comments based on existing JTC1/SC32 standards developed during the past decade. As such the ballot comments made below are based on 1) generic ISO/IEC JTC1/SC32 standards pertaining to electronic data interchange (EDI) among Persons, i.e., as entities which can make (legal) commitment, be held accountable, etc., based on laws and regulations of applicable jurisdictional domains. Of particular relevance here are three generic ISO standards which one needs to take into account and be harmonized with in the development of any new ISO standard which pertains to both EDI and/or privacy protection, namely, *a)* ISO/IEC 14662 "*.Open-edi Reference Model*[2]*";* b) ISO/IEC 15944-1 ". *Business Operational View- Part 1: Operational aspects of*	TC 215 Project Editor(s) and experts working on the TS 14441 project are requested to download the "freely available" standards noted here so that they have them (and the text they contain) available for reference and use at the ballot resolution meeting for TS 14441.	

[2] ISO, IEC, ITU and UN/CEFACT agreed over a decade ago that the ISO/IEC 14662 "Information technology – Open-edi reference model" should serve as the common generic base standard for any ISO standards involving EDI, i.e., any electronic data interchange among autonomous (legally recognized) entities. This high level standards (legal) agreement among ISO, IEC, ITU, and UN/FACT led to the "MOU on MoU on electronic business between IEC, ISO, ITU, and UN/ECE" {See further < http://www.itu.int/en/ITU-T/ebusiness/Pages/mou/mou.aspx >.

[3] The ISO/IEC 14662 "Open-edi Reference Model" was developed in 1995 by the former ISO/IEC JTC1/SC30 "Open-edi" based on a "conceptual model" developed by its predecessor ISO/IEC JTC1/WG3- Electronic Data Interchange (EDI). Currently ISO/IEC JTC1/SC32 basically maintains the Open-edi reference Model, there not being any need for technical changes. ISO/IEC 14662 (3rd edition) is a freely available ISO standard {See further, {see further www.iso.org/PubliclyAvailableStandards }.

				Open-edi based implementations" 2) ISO has made these three generic EDI standards "freely available" as they are to serve as base generic standards for reference and use in particular fields of application of IT. {see the "*MoU on electronic business between IEC, ISO, ITU, and UN/ECE" at* <http://www.itu.int/en/ITU-T/ebusiness/Pages/mou/default.aspx> 3) In addition, one notes that JTC1/SC32 from its inception has maximized identification, reference and re-use of existing ISO standards as much as possible. As such as the above referenced ISO standards, identify, reference, and use near fifty (50) existing ISO, IEC, ISO/IEC and ITU standards. 4) Based on the above approach, JTC1/SC32 developed its ISO/IEC 15944-8 "…*Business Operational View – Part 8: Identification of privacy protection requirements as external constraints on business transaction".* **Note: A copy of this IS standard has already been provided to TC215 via an earlier liaison contribution.** 5) One assumes that "health informatics" is a particular IT field. and as such ISO/TC215 will benefit from		

				a) basing its further standards development from the technical comments made below; and, b) maximize use of existing ISO concept/definitions as is or as adapted 6) In addition, it is noted that JTC1/SC32 in its maintenance[3] of its "Open-edi reference model" has focused primarily of the generic business operational view family of standards, maximizing use of existing ISO standards when and where applicable, including those of TC 215.		
SC 32-07	Clause 1	Scope	te	A detailed analysis of the Clause 1 Scope statement has brought forward a number of comments which are presented below.	One trusts that the comments SC32 06, 07 and 08 will assist in clarifying some aspects of IS 14441 and resolve some apparent technical issues.	
SC 32-08	Clause 1	Scope	te	Focus on "privacy" and reference existing TC211 and ISO, ISO/IEC, IEC and ITU standards with respect to security requirement. On the whole, privacy protection requirements are of accountability, information/data management, and interchange in nature. Security aspects are minor and of a safeguarding nature. Further security services and techniques are of the nature of a functional support service, i.e., used to support (explicitly stated) information/data management and interchange requirements whose implementation requires the invocation and use of specified security	1. In the context of the Clause 1 Scope statement stating that "security management is included in the scope of ISO 27799", it is highly recommended that TC211 maximize the use of this existing IS standard of TC 211 in the completion of its work on this TS. This will maximize interoperability of the new TS with an existing TC211 standard. It will also avoid overlap and duplication of the proposed new TS with ISO 27799. Further any use or implementer of the new TS 14441 would also need to reference and use ISO 27779.	

				services and technologies and relevant/applicable ISO, ISO/IEC, IEC and ITU standards in support of the same. Here one notes that the last sentence of the Scope statement, which focuses on exclusions to the Scope of TS 14441 references ISO 27799 which deals with "*Information security management in health".* The current ballot document for TS 14441 does not appear to identify any information security management requirements which are not already addressed via its TC215 ISO 27799 standard. If it does these should be identified and made explicit in a separate Clause or sub-Clause. Here it may well be that information security management in health services which are optional or conditional in a generic health services context including their IT systems would be mandatory when personal information of patients (including their Hers).	Based on the assumption, that TC211 supports this approach, it could take the following steps, which would not only improve the current draft for TS 14441 but also maximize interoperability with existing ISO 27799, a) identify specific demands for types of security services arising from privacy protection requirements which are not already covered and provided for in its ISO 27799 "Information security in health" standard; b) that should any such additional information security services be identified as need to support privacy protection requirements, that TC 211 decide whether or not the best way to handle these via an amendment to ISO 27799, i.e., especially where these are deemed to be part of "generic" best information security practices. c) that one consider, adding a Normative (or Informative) Annex to TS 14441 which identifies specific information security services required to support privacy protection requirements and then map these to ISO 27799.	
SC	Clause 1	Scope	te/ed	Given the comments made above and the fact	Consider removing "security" from title,	

32-09				that security services are but a subset of all the privacy protection requirements which are of the whole ore of an information management, data interchange and accountability in nature, one should consider removing “security” from the title and focus on privacy protection.	focus on privacy protection and reference and make extensive use of TC215’s ISO 27799 Information security management in health standard.	
SC 32-10	Clause 1	Scope	te/ed	The last paragraph contains a number of exclusions. It is important that these be made clear, (e.g. via a new sub-Clause in Clause 1). It is not uncommon for ISO standards to have two or more subclauses in it Clause 1 Scope. For example, Clause 1 Scope Clause 1.1 Statement of Scope Clause 2 Exclusions Clause 3 Aspects not yet addressed[4]	Consider taking text of the first four paragraphs and place it under Clause 1.1 Statement of Scope; And then take the text of the last paragraph, as is or as amended, and place it under Clause 1.2 Exclusions	
SC 32-11	Clause 2	Normative references	te/ed	1. There are Normative References which are used several times in the document but not yet included in Clause 2 (e.g. Guide 73, ISO 9000, etc.) There may be others (e.g. ISO 17065 is referenced in Clause 6.1 but its title in not found in either Clause 2 or the Bibliography.	Project Editor requested to review next version of this document and add entries to Clause 2 accordingly, i.e., references in normative text, including Clause 3, to other ISO standards, and/or update the Bibliography.	

[4] “Aspects not yet addressed”, if often used when one is working on a 1st edition of a standard focussing on key primary (or primitives) first and then based on implementation and practice develop those other aspects either in the 2nd edition or via a Part to the standard (in the context of a multipart standard)..

SC 32-12	Clause 3	All	te	1. ISO/IEC JTC1/SC32 notes that the current ballot document for ISO/TS 14441 is "non-conformant" with ISO Directives with respect to formatting and presentation of definitions of concepts. A key requirement of ISO Directives is that any character string(s) or word (or set of words) which is intended to be used as a "term", i.e., representing the designation of a concept defined in a Clause 3 entry shall be indentified as such. by being represented in either bold or *italicized"* form.	JTC1/SC32 liaison requests that the next version of Clause 3 of this document in the text of the definitions that words which are used as terms (representing defined concepts), be so identified , as per ISO Directives.	
SC 32-13	Clause 3.1	accounta-bility	Te	"**individual**" and "**organization**" are recognized and widely used ISO standard defined concepts as sub-types of "Persons" and as defined can be held " However, one is not sure what is meant by the use of the word "community" which appears to be intended to have some meaning. That is, how and in what way does one define "community" and in a manner In which it can be held "responsible"?	JTC1/SC32 liaison in noting that "accountability" is its privacy protection principle #2 {See Clause 5.3.2 ") requests TC215 to consider to change the text of the proposed definition for the concept of "accountability" to delete "community" and replace it with "public administration". A primary reason here is that one cannot hold a "community" "accountable." Should TC/215 decide that the concept of "community" is important, it needs to be defined.	
SC 32-14	Clause 3.2	access control	Te	1. Consider replacing "data processing system" with the ISO concept and definition of "information technology" (IT system) which is more generic and covers any kind of recorded information". One reason is that privacy protection requirements apply to both hard-	1. Recommend using, and adding to Clause 3, the existing ISO definitions for **information technology system (IT system)**	

Timothy Schoechle 3/6/13 1:10 PM
Comment: Spelling?

				copy records and soft-copy records, i.e., all types of recorded information about an identifiable individual. 2. Replace “entities” with “Persons”. This will reduce confusion with the existing ISO generic and widely used definition of “**entity”** in all field of use of ITC namely, **entity**	**recorded information** 2. The resulting draft definition would be: ***access control*** *procedure(s) for ensuring that the contents, i.e., **recorded information**, in an **information technology systems (IT system)** can be accessed only by **Persons** as formally so authorized by the **organization** of which the **IT system** is part*	
SC 32-15	Clause 3.3	accredita-tion body	Te	1. The proposed definition appears to be an expansion the term. It is not clear what “accreditation” is and for what. 2. The Note indicates that an accreditation body derives its “status” and role via a jurisdictional domain of which it is part. This also implies that the remit of that accreditation body is linked to that of the relevant jurisdictional domain. This can be at the state or province level, the national level, the regional level (e.g. the EU) or international level (e.g. World Health Organization (WHO)). 3. To address this generic requirement the concept and definition of “jurisdictional domain” was developed (e.g. the EU is not a “government” but functions as a	1. JTC1/SC32 liaison recommends a) adding the existing ISO concept and definition of “jurisdictional domain” to Clause 3 and using it throughout the document where and whenever applicable b) consider the following revised draft definition **accreditation body** **Person** authorized by the applicable **jurisdictional domain** to undertake accreditation services and issue accreditation credentials to an **organization** or **public administration** as specified by that **jurisdictional domain**	

				jurisdictional domain). Here for all EU nation-state members, the primary source of external constraints specifying privacy protection requirements is its Directive 95/46/EC. 4. The existing ISO definition of for the concept of "**jurisdictional domain**" is **jurisdictional domain**	c) ISO TC 215 to develop a definition for the concept of "accreditation"	
SC 32-16	Clause 3.4	anonymi-zation	Te	1. JTC1/SC32 also used the ISO TC215 standard ISO/TS 25237 definition for "anonymization" and adapted it in the context of privacy protection requirements which apply not just to "data" but also "hard copy" records. To address this privacy protection requirement, ISO/IEC JTC1/SC32 adapted the ISO/TS definition as follows: **anonymization** **process** whereby the association between a **set of recorded information (SRI)** and an identifiable **individual** is removed where such an association may have existed NOTE Adapted from ISO/TS 25237 [ISO/IEC 15944-8::2012 (3.3)] 2. In this context, and to address other data management and interchange issues as well, JTC1/SC32 introduced the concept of "**set of recorded information**" [for text see Clause 3. 3.121 in ISO/IEC 15944-8]	1. JTC1/SC32 recommends that TC 215 in its further work on the ISO/TS document consider a) using the adaption of the TS 25237 definition of "**anonymization**" developed by JTC1/SC32 in a privacy protection context and provided here; and, b) add the concept/definition of "**set of recorded information**" as is, or as adapted, this being very relevant to EHR systems.	

				3. Here it is useful to highlight the fact that SRI is a dynamic concept and links directly to the manner in which an organization decides to manage and control its recorded information. An SRI can pertain to a single data element, or the complete health record of an individual. It can pertain to any part of the individual's health record (e.g. an X-ray, an MRI scan, a blood test, etc.). Here for each of these discrete SRIs different access and use controls will apply to various Persons depending on their roles and responsibilities in medical procedures and treatments. Further an SRI can consist of one or more other SRIs.		
SC 32-17	Clause 3.5	asset	Te	Question: In the context of privacy protection requirements, a SRI on identifiable individual, and/or personal information on that individual may be of value to that individual but not to the organization which controls such personal information. Also in the context and focus of privacy protection requirements, one could consider a patient HER to consist of various sets of recorded information (SRIs), some of which contain do not, while those SRIs which contain personal information differing access, use, life cycle, interchange, etc., conditions apply.	Consider using "personal information asset" instead or as an added concept/definition here. the key concept/definition here. Here follows a draft definition: ***personal information asset*** *any **personal information,** or part thereof, about an identifiable **individual** considered to be of value to the controlling **organization** or **public administration** and/or the **individual** to whom it pertains*	
SC	Clause 3.6	assurance	Te	Question: Security services and standards do	Consider separating	

32-18				not address assurance requirements pertaining to the contents, i.e., recorded information in an IT system. Privacy protection requirements are primarily about accountability and management of the personal information in the IT system(s) of an organization or public administration. One can therefore have very good security management but not very good information management (and vice-versa).	1) assurance of information management of personal information which is "content" focused from 2) assurance of management of security services which on the whole are functional support services to information management and governance requirements.	
SC 32-19	Clause 3.7	attestation	Te	An "attestation" pertains to documenting of providing or serving a clear evidence of that which is being attested to. Also an "attestation" can only be made by a Person." In addition, since "attestation" has defined meaning in law in applicable jurisdictional domains, One should consider using a "qualified" term for this concept, such as "conformance attestation". This is already stated as a NOTE for the Clause 3.8 definition for "audit".	Consider incorporating these attributes into a revised definition. Possible draft text **"conformance attestation** Issuance of a recorded statement by a **Person**, so qualified, based on a decision by that **Person** following review that a specified set of requirements have been fulfilled and so clearly demonstrated."	
SC 32-20	Clause 3.9	availability	Te/ Ed	Based on comments elsewhere, re proposed new ISO TC 215 definition of the existing ISO concept/ definition of "entity", recommend that "entity" be replaced by Person, since this appears to be what is intended.	Recommend replacing "entity" with "**Person**".	
SC 32-	Clause 3.12	confidentiality	Te	1. It is assumed that by use of "information" in the text of this definition what is really meant is	1. Consider replacing in text of definition "information" by "recorded information" in	

21				"recorded information", i.e., EHRs by definition contain only "recorded information", i.e. spoken comments in the provision of health services which are not "recorded" therefore cannot exist in EHRs. Here an audio recording is a type of recorded information. Further privacy protection requirements apply only to recorded information. 2. The phrase "unauthorized individuals, entities, or process" raises some ambiguity. In health services (and generally) in IT systems) authorized access is often provided at the organization part or IT system level as well as to specific sub-sets of the complete HER. Further a "process" can only be invoked by a Person. Also the text of the current definition contains two negatives.	this definition and throughout the document as applicable. This will provide some clarity. 2. In light of other comments re use of Person, entity, IT system, etc. consider draft replacement text as follows *"property that assures that recorded information identified as confidential is not accessible or made available to any Person (or IT systems of that Person) without that Person having a clear and well-defined authorization for access to recorded information* *NOTE A Person authorized to access a specified kind or set of recorded information shall commit to a written undertaking to maintain the appropriate confidentiality requirements including those of a non-disclosure nature.*	
SC 32-22	Clause 3.13	confor-mity assess-ment	Te/ Ed	The definition contains the text " .. person or body..". "Body" is not a defined concept in this document (as well as in the context of EHRs usually refers to a "dead individual"). If what is intended by "body" is any	Consider replacing "..person or body.." with "..Person.."	

				organization or public administration", then this is incorporated in the definition of "Person"		
SC 32-23	Clause 3.15	data subject	Te	JTC1/SC32 is well aware of the EU Directives on data protection and made it a Normative Reference in the development of its ISO/IEC 15944-8 ".privacy protection.." standard. However, what is intended here is not "person" (or "Person") in general but that of an "individual". Further as already noted, privacy protection requirements apply to both hard-copy and soft-copy forms of recorded information[5], including any printouts of an EHR, as stated in this document. Further the NOTE seems also indicate that "individual" is what is intended and not persons in general (including as group).	1. Recommend that TC215 consider amending the text for this definition as follows "individual to whom the **recorded information** refers". 2. Also note that "data subject" is an EU specific context and not international in nature (e.g. not used in the USA, Canada, Australia, the APEC Privacy Framework, etc.). Since TS 14441 focuses on clients of a health care service, and these by their very nature are "patients", one should consider replacing "data subject" with "patient".	
SC 32-24	Clause 3.16	entity	Te	It is noted that ISO/TS 14441 makes use of the ISO/IEC 2382 series of information technology vocabulary standards. This standard does have a definition for "entity" which is widely used, in all areas of application of information technologies and based standard development committees. Its definition is as follows:	Consider adding and using this existing ISO/IEC definition of "entity" as a general reference to any type of entity and then "Person" in this document when one is actually referring to a natural or legal person.	

[5] Early European Data Directives and OECD Guidelines in the early 1980's focussed on "data", as that found in IT systems only. This was one reason in Europe one still often refers to "data protection". However, in most countries and now also in the EU "privacy protection" is used to reflect the fact that it pertains to personal information on or about an identifiable individual, irrespective of its means of recording, process, or interchange.

				entity any concrete or abstract thing that exists, did exist or might exist, including associations among these things EXAMPLE A person, object, event, idea, process, etc. NOTE An entity exists whether or not data about it are available or not. [ISO/IEC 2582-17:1999 (17.002.05)] [for text see Clause 3.3.44 in ISO/IEC 15944-8]		

SC 32-25	Clause 3.17	first-party confor-mant assess-ment activity	Te/ Ed	1. Use of the phrase “person or organization”. An organization is a Person. It appears that when it is the intention to cover all kinds of persons, one should use “Person”. 2. Ii is not clear, why this concept/definition is needed in a Normative matter. It appears to be used only once in the Normative part of the document, i.e., in Clause 6.1 where this definition is basically repeated although with other text (This needs to be harmonized). Further it is used in Annex A which is an informative Annex related to the conformity assessment of a `”product”. However, in the context of TS 14441, it is not clear as to what is the “product” to be assessed (The Clause 3.42 definition for “product” does not help here either).	1. Recommend replacing “person or organization” by “Person” in the text of this definition. 2. Need a serious re-think here as to what is a “product” in a TC211 TS 14441 context. One assumes that this is to be an EHR of an organization whose PHI is managed in compliance with applicable privacy protection requirements, but this is not made clear in the current version for TS 14441 and needs to be addressed and resolved before this document is progressed further.	

SC 32-26	Clause 3.18	health informa-tion system	Te/ Ed	As per other comments above, replace "information" with "recorded information". It is also assumed that by "subject of care" one refers to an "individual". If this is so a "health information system" is that part of the IT system(s) of an organization which has applications which contain personal information. It is not understood of what is meant by "transmitted securely". Should there not be a reference here to a specific clause in ISO 27799 The whole set of information management and change management requirements are missing, i.e., is more than a repository. Further, the text of the existing definition contains some attributes of a conformance nature but leaves out others. It is better not to have any "requirements" here on a partial basis (else one should include them all)	TC215 to consider and decide whether or not in this standard, one needs to make a differentiation or distinction between those applications in the IT system(s) s of an organization which manage personal information and which do not. If this is the case, one should consider that following draft revised text **health information system** **(HIS)** application(s) in the IT system(s) of an organization or public administration which contains personal information on an individual as subject of care *NOTE 1 A health information system of an organization or public administration, as well as the electronic health records (EHR) which it contains, should be able to be conformant to applicable privacy protection requirements, subject to the laws and associated regulatory privacy protection requirements of the applicable jurisdictional domain(s).* *NOTE 2 = existing NOTE 1 text* *NOTE 3 = existing NOTE 2 text*	

SC 32-28	Clause 3.21	health profess-sional	Te/ Ed	Can only individuals be health professionals, or can organizations and/or public administrations also be health professionals? The reason for this question is the use of "person" in the definition. Another question: It is assumed that who or what is an "authorized body" is determined by the rules governing qualification & accreditation of a "health professional" in the relevant/applicable jurisdictional domain(s) Further this definition needs to be place in the context of this standard with respect to personal information	Based on the comments made, the following draft revised text serve as an input to a revised definition **health professional** **individual** who is accredited and so registered, via a recognized **organization** or **public administration**, in the applicable **jurisdictional domain(s)** as qualified and so authorized to perform specific **health care** activities NOTE 1 Associated with the type and nature of an authorized health professional are associated access and use of personal information privileges and privacy protection requirements pertaining to personal information of any individual Amend existing NOTES 1 & 2 accordingly.	
SC 32-29	Clause 3,23	identify-able person	Te	Taking into account here the reference to the Directive 95/46/EC, which JTC1/SC32 cited as a Normative reference in Clause 3 of its generic ISO/IEC 15944-9 ".privacy protection..", and, also already keep in mind when developing in late 1990/early 2000 Part 1 of the multipart ISO/IEC 15944 standard, it was clear that this EC Directive pertained not to persons in general but that the reference here is to a person as "individual" and not as an "organization". A key reason here is that in many jurisdictional	1. Recommend to TC 215 that it amend the current text as provided below ***identifiable individual*** *any **individual** who can be identified, directly or indirectly, via **recorded information** or or about that **individual,** in particular by reference to an identification number or via any **recorded information** pertaining to one or more properties particular to the individual with respect to those which are physical, mental, economic, cultural societal, etc. in nature.*	

				domains the use of “person”, refers (or can refer) to any legally recognized entity, i.e., an individual, organization, public administration, etc. This causes confusion. And since privacy protection requirements are invoked and apply only with respect to recorded information on or about an identifiable individual, i.e., ‘’personal information’’. The ISO/IEC 15944-8 standard supported this EC definition in the development of the new definition of “personal information” [for text see Clause 3.99 in ISO/IEC 15944-8].	*NOTE Adapted from the “EU Directive 95/46/EC* on the protection of individuals with regard to the processing of personal data and on the free movement of such data”*. and positioned in an international privacy protection requirements environment.*	
SC 32-30	Clause 3.24	identifi-cation	Te	1. The current proposed definition is ambiguous. It does not provide any criteria for “recognition”. In addition, “recognition” is linked to recall and based on information or knowledge already available that individual. Nor does this definition, address the question of “recognition” by whom?	1. TC215 is requested to consider differentiation between “identification”, as a rule-based process, and “identifier” as the result of the application of such a process. A key criteria for any EHR ISO standard in support of privacy protection requirements should be supporting the unambiguous identification of any individual registered in an HIS including ensuring that applicable information management, accountability and security Requirements of a privacy protection nature are implemented.	

[6] This is a freely/publicly available ISO standard.

				2. In its ISO/IEC 15944-1 standard development, JTC1/SC32 participants spend considerable time and resources early in 2000"s to address and resolve issues associated with "identification" in a very logical and systematic manner, maximizing use of existing ISO standards which had already addressed various issues pertaining to "identification" and the assignment of resulting "identifiers. The results are found in (2nd edition) ISO/IEC 15944-1:2011[6], *Annex C (informative) Unambiguous identification of entities in (electronic) business transaction*", and *Annex D (Informative) Existing standards for the unambiguous identification of Persons in business transactions (organization and individuals) and some common policy and implementation considerations.* The most significant results were the findings and recognition that a) "identification" is a rule-base process whose purpose is to assign and register an unambiguous identifier an entity being identified as such; and, b) any entity, and especially a Person will likely have one or more unambiguous identifiers, [for text see Clause 3.53 for the ISO definition of "identification" and Clause 3.54 for the definition of "identifier" in ISO/IEC 15944-8]	2. In particular, TC215 Project Editor, and participating experts are requested to familiarize themselves with Clause 8 in ISO/IEC 15944-8 which addresses, resolves and provides solutions to issues pertaining to unambiguous identification of individuals as well as the assignment of unambiguous identifiers.	

				3. Further it needs to be noted that any Person and especially an individual" may have multiple valid identifiers and associated identities. However which of these are "recognized personal identities (rPi)" is another matter. Clause 8 *Principles and rules governing the establishment, management and use of identities of individuals*" in ISO/IEC 15944-8 are very useful here and of particular relevance to further development of the ISO/TS 14441 standard. 4. In addition, one should note and highlight that the <u>name</u> of an individual cannot and does not serve as an "identifier". It is simply a "persona". An individual will have many personae and may well have more than one "legally recognized name" (LRN). Issues of this nature are addressed and resolved in Clause 9.3 "*Personae and legally recognized names (LRNs) of an individual"* of ISO/ IEC 15944-8.	3. In addition, one should note and highlight that the name of an individual cannot and does not serve as an "identifier". It is simply a "persona" used by the individual in a (specified) context. An individual will have many personae and may well have more than one "legally recognized name" (LRN). 4. Consider introducing and adding the concept and definition of "persona" (as defined in Clause 3.48 of ISO/IEC 15944-1:2011 (2nd edition) as **patient persona** set of data elements and their values by which a **patient** wishes to be known and thus identified and is so recorded n a **health information system** NOTE 1 The same individual may well have multiple name representation, some of which are legally recognized names. NOTE 2 The health information system of the organization or public administration usually assigns its own identifier to a patient, independent of other identifiers or other persona which	

					an individual may have.	
SC 32-31	Clause 3.24	identifica-tion	te	1. It is assumed that this definition focuses on an individual only and not `person` in general, i.e., also organizations, public administration. 2. Identification is a process which results in the assignment of an identifier, `recognition` as in this document. Given that the definition of the concept stays the same (apart from changing `person`` to “individual”), consideration should be given to assigning a more appropriate label as term for this concept/definition pair, e.g. “identified individual”.	1. Change “person” to “individual”	

SC 32-32	Clause 3.25	information governance	Te	1. The proposed definition here is not linked to privacy protection requirements. 2. The proposed definition does not cover or include fiduciary, evidentiary and other relaxed legal requirements pertaining the recorded information of an organization or public administration. On the whole the use of the general use concept of "governance" pertaining to an organization or public administration includes the need assure that any governance principles rules of an organization are in compliance with and support laws and pursuant regulation of the applicable jurisdictional domain. 2. In addition, a search on the use of this concept in the existing document, indicates that it is used on an Annex A (informative) and not in any text of Normative Clauses in ISO/TS 14441. It is not a good ISO practice to include in Clause 3 a normative Definition if it is only used in informative text.	Recommend that TC 215 consider deleting Clause 3.25 unless in its next version the concept of "information governance" is used in text of a Normative Clause.	
SC 32-33	Clause 3.26	information privacy	Te	1. On the whole privacy protection is a legal construct introduced in various jurisdictional domains during the past two decades as consisting of a) a set of rights of an individual with respect to its personal; information; and b) a set of obligations of organization and/or public administrations which collect/create,	Proposed revised text for TC 215 to consider here is the following **personal information privacy(PIP)** combination of the set of rights of an **individual** and concomitant set of obligations of an **organization** or **public administration** with respect to the	

				manage, interchange, etc. personal information. The current proposed definition for information privacy does not make such a distinction. It should. Also privacy pertains to “personal information” (only). So a more appropriate assigned term here would be “personal information privacy (PIP)”. The proposed revised draft definition will map to and is harmonized with Privacy principles of the Accounting bodies. Referenced.	collection/creation, management, access and use, retention, disclosure (electronic data) interchange and disposal of **personal information,**	
SC 32-34	Clause 3.27	informa-tion security	Te	1. One notes that the ISO/IEC 27000 – Security techniques standards series in their use of in the title of “Information security” basically focus on protecting the “contents” of the recorded information in a “container”. They do not, nor are intended to address, privacy protection requirements which on the whole are of an information management and accountability nature with respect to ensuring the timeliness, accuracy and relevancy (= integrity) of any personal information in an EHR. As such ISO/IEC 27000 standards do not (and were never designed or intended) to pertain to/address information/records manage requirements, including change management of the recorded information in any (health record) or set of recorded information of an organization or public administration.	In response to the comments made here the following solution is offered 1) differentiate between the concept/definition of information security and information integrity; and, 2) change the current proposed definition for information security to read as follows, **information security** set of defined rules and associated processes of an **organization** or **public administration** pertaining to the assurance of confidentiality**,** access, and	

				2. One solution here would be to make a differentiation between a) information security; and b) information integrity.	data interchange controls of **personal information** **information integrity** set of defined rules and associated information management process of an **organization** or **public administration** pertaining to the assurance that any **personal information** under the control on an **organization** or **public administration** is relevant and kept timely and accurate	
SC 32-35	Clause 3.28	inspection	ed	The use of the word `person`` seems out of place in the NOTE, unless what is intended is an `"organization``	Recommend that in the NOTE, one delete "person" or replace by "organization"	
SC 32-36	Clause 3.29	personal health informa-tion (PHI)	te	The use of "person" in the definition seems out of place, especially since individual is used twice in the same definition. This may cause confusion.	In order to have a consistent approach in the definition change "person" to "individual"	
SC 32-37	Clause 3.31	point-of-service (POS) clinical system	ed	The use of the qualification "that is used by end-users" raises some questions and ambiguities, including "What or who is an end-ser?" Is the phrase necessary?	Consider rephrasing the start of the definition to read as follows: "system that is used at a point of care or service……."	
SC 32-38	Clause 3.32	privacy breach	te/ed	A privacy breach is or should be more that a "processing". It also includes access, use, management, interchange, " This is also important considering that Clause	Consider strengthening and making more complete this definitions by replacing "processing" with "accessed, processed, managed, disclose or interchanged in an unlawful manner…"	

				3.33 privacy control is based on 3.32 See also below comments on Clause 3.40 processing of PHI		
SC 32-39	Clause 3.33	privacy control	te	One would assume that this would be a positive concepts and not a risk minimization approach, i.e., in the context and approach that privacy controls are directed at preventing privacy breaches, i.e.., as safeguards.	Consider a positive preventive approach by defining the concept of "privacy control" as : "technical and organizational measures aimed at ensuring that privacy breaches do not occur	
SC 32-40	Clause 3.34	privacy policy	te	There is a need here to link the definition of this concept to privacy protection requirements. There is also a need to link this concept to a responsibility of an organization. See also the comment above on Clause 3.32 and 3.33 above	Consider strengthening this definition (taking into account comments above. Here is suggested draft text: *"specification of objectives, rules, obligation and privacy controls established by an organization in support of applicable privacy protection requirements with respect to creation, management, access and use, disclosure or interchange of PHI in a particular context.*"	
SC 32-41	Clause 3.35	privacy preferenc e	te	An individual's privacy preference usually pertains to who uses or has access to PHI, disclosure and sharing of PHI. On the whole an individual is not that familiar with PHI (data) processing. Further, issues of this nature are usually covered under "informed consent". Also "informed consent" is exactly that, one cannot have "implied consent".	Consider clarifying and strengthening the definition for this concept. Here is some draft text: "*specific choices made by an individual among the choices available with respect option on use, disclosure or sharing of PHI in accordance with applicable privacy protection requirements.*	

				Is it the intention to ascertain privacy preferences from the individual concerned as part of an “informed consent” process?		
SC 32-42	Clause 3.36	privacy principle	te/ed	1. Clause 5 in ISO/IEC 15944-8 it titled “Fundamental principles and assumptions governing privacy protection requirements…”. It contains 11 Privacy Principles. The integrate and consolidate those of the OECD Guidelines, the EU Directives, the APEC Privacy Framework as well as those found in national legislation. 2. It is assumed that the set of privacy principles is established by an organization which holds or controls PHI. This needs to be made clear. In addition, privacy protection requirements, apply to both data and hard copy documents, i.e., any “hard copy” inputs or outputs from an ICT system. This also needs to be made clear.	1. Consider adding an EXAMPLE which reads as follows: EXAMPLE For an example of set of privacy protection principles integrating existing world-wide requirements, see ISO/IEC 15944-8, Clause 5 “Fundamental principles and assumptions governing privacy protection requirements..”. This is a freely available ISO standards `(see further < http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html > 2. Recommend strengthening and clarifying the definitions here as follows: “*set of shared rules and values of an organization governing the privacy protection of any PHIs held by or under the control of that organization, including that in its ICT systems*”	
SC 32-43	Clause 3.37	privacy risk asses-ment	te	This definition is depended on the definition of “privacy breach” (See our comments on Clause 3.32 above) as well as “processing” (see Clause 3.40 below)	Change “envisaged processing operation” to envisaged PHI processing operation”	

SC 32-44	Clause 3.38	privacy safeguard measures	te/ed	Comments similar to that in nature as those above for Clause 3.33 privacy control, i.e., to take a positive approach	Suggest redraft text to read as follows: " criteria to be fulfilled when implementing privacy controls designates to ensure that privacy breaches to do occur"	
SC 32-45	Clause 3.40	process-sing of PHI	te	A number of comments were made above with respect of the use of the word "processing" by itself, i.e., in its common English language use. These comments could be resolved by changing the label assigned to this definition from "processing of PHI information "to that of "PHI processing" as a term.	Suggest solution and approach 1. Change to term for Clause 3.40 definition to "PHI processing". This will also improve understanding and readability of this standard, and make the use of the term "PHI processing" synonymous with application of privacy protection requirements in a health informatics use context. 2. Throughout the standard, including in Clause 3 text of definition where "processing" is used change and replace by "PHI processing" and use as a key term throughout the document (including Annexes). 3. Consider amending the definition for "**PHI processing**" to read as follows: "*any operation or set of operations performed on the contents of PHI, including collection/creation, storage, access and use, analysis, linkage, communication, disclosure and retention, within an organization as well as data interchange with any other Person"*	
SC	Clause	profile	te/ed	1. Profile is a generic concept while that which	1. Change "profile" to "patient profile".	

32-46	3.41			is intended in Clause 3.41 pertains to profile of an individual. Also this concept needs to/should be defined in a `health informatics" context (and not "profiling" in general). Further an individual may well have, and often does have within a health service, several different and distinct profiles where the PHI these individual profiles contain may well not be shareable within an organization (e.g., a psychiatric or mental health assessment, etc.) 2. Further, a "profile" often is not "automatically generated" but is often the result of analysis of PHI entered into an ICT system based on applicable rules and supporting algorithms, etc. The definition and use of this concept needs to be clarified and strengthened accordingly. 3. The Clause 0 Introduction uses ''protection profile''' and Clause 4 includes PP as the abbreviation for ''protection profile'' but the rest of the document appears to have no mention of protection profile or what it is. However, the indication of the text in the document appears that ''profile'' relates to that of a ''patient''.	2. Consider amending text of the definition to read as follows **patient profile** **PP** "*result of analysis of the **PHI** of an **individual** as patient generated based on predefined rules and algorithms for the purpose of categorizing **individual** and to be applied to that **individual** in the provision of **health care** services* *NOTE 1 A patient profile is used for the purpose of analyzing or predicting personal preferences, behaviours and attitudes, possible medical treatments and post-care services.* *NOTE 2 Within an organization, an individual may have as part of its EHR, more that one patient profile as sub-sets of its HER. Here there may be specific added access and use controls of the PHI in such patient profiles.*	
SC 32-	Clause 3.42	product	te/ed	It is assumed that related to a particular process the end result is a specified, or expected product. Here the use of the ISO	1. Consider deleting Clause 3.42 and renumber remaining Clause 3 entries	

47				9000 Clause 3.4.2 definition, in ISO 9000 is predicated on and based on the ISO 9000 Clause 3.4.1 definition of the concept of "process". Here this standard has a new and defined concept of "PHI processing". Further, ISO 9000 definition for the concept of "product" have voluminous NOTE text associated with it. If in this TS 14441 the focus is on privacy protection requirements for EHRs containing PHI, the question is asked whether one needs to or should define "product" at all in this standard	accordingly. 2. If Clause 3.24 concept & definition for "product" is to be maintained, one needs to add/insert the ISO 9000 3.2.1 definition for "process".	
SC 32-48	Clause 3.43	pseudonymization	te	1. JTC1/SC32 in its development of its privacy protection standard, ISO/IEC 15944-8 used and referenced the ISO TC215 standard ISO TS 25237 "*Health informatics-Pseudonymization".* This resulted in the inclusion of the following two concepts and their definitions in its Clause 3, **3.113** **pseudonym** use of a **persona** or other **identifier** by an **individual** which is different from that used by the **individual** with the intention that it be not linkable to that **individual** NOTE Adapted from ISO TS 25237 **3.114**	1. TC 211 is requested to apply, reference and make use of its existing ISO TS 25237 standard on "Pseudonymization" (as JTC1/SC32 did). Here in an ISO/IEC 15944-8 eBusiness & privacy protection standard an "alias" is a particular sub-type of "persona". 2. JTC1/SC32 to ISO TC 211 liaison is prepared to assist here.	

				pseudonymization particular type of anonymization that removes the association with an **individual** and adds an association between a particular set of **characteristics** relating to the **individual** and one or more **pseudonyms** NOTE Adapted from ISO TS 25237 2. The purpose of pseudonymization (as per existing TC 215 ISO TS 25237 is to remove "linkability" The proposed Clause 3.43 does not do this		
SC 32-49	Clause 3.44	review	te/ed	The assignment of the word "review" as the label or term for this concept. What seems to be intended here is a "conformity assessment review" (CAR)	For greater clarity and reduce ambiguity, consider 1. changing the label for Clause 3.44 from "review" to "conformity assessment review" (CAR); and, 2. add the acronym CAR to Clause 4 and use "CAR" (or "conformity assessment review") throughout the document.	
SC 32-50	Clause 3.51	second party conformity assess-ment activity	te	See comment above on Clause 3.17 An organization is a Person, therefore the use of 'organization' in the NOTE is redundant	Resolve as per Clause 3.17 Change NOTE to read "A Person performing second-party …."	
SC 32-	Clause 3.52	secondary use	te	This concept does not appear to be used anywhere in the existing TS 14441 document	Either use the concept of "secondary use" in normative text for the next version	

51				and thus should be deleted	of this document or, if not, delete.	
SC 32-51	Clause 3.54	subject of care patient	te	1. Reviewing the current version of TS 14441, the term “patient” is used throughout and that for “subject of care” only rarely, i.e., almost only in Clause 3. Also the use of the term “patient” is much more closely linked to a health service than a “subject of care” which is also use in many non-health environments (e.g., day care, social services, etc.). Also the term ”patient” links more closely and better to HER and PHI than the more generic concept of “subject of care. 2. More importantly an ISO definition needs to be stated in the singular, the associated labels are. Also a “person” can be an organization	1. Recommend that “patient” be the main term associated with this concept and “subject of care” more that of a synonym. 2. Have the text for the definition in the singular and use “individual”. 3. Consider using the following (draft) replacement text: **3.54** **patient** **Individual** scheduled to receive, receiving or having received a health service from an identified **health organization** or **health professional** NOTE 1 Within a health organization a “patient” is sometimes referred to as a “subject of care”. NOTE 2 Adapted from ISO TS 18308:2011 (3.47)	
SC 32-52	Clause 3.55	system integrity	te	One could not find any use of the concept of ‘system integrity’ in the normative text for this document. Further in a privacy protection requirements context the concept of ‘data integrity’ and its definition would be much more relevant and useful	In the next version for TS 14441 use ‘system integrity’ in a meaningful way in Normative text, or else delete from Clause 3	

SC 32-53	Clause 3.56	target of evaluation TOE	te	1. The proposed definition does not make much sense in a privacy protection requirements context which is one which focuses on an EHR or a PHI within an EHR. Consequently one would expect a TOE to be directed at and concerned with the data integrity of PHIs within the ICT systems of an organization. 2. Further, one finds in Clause 5.4 Common Criteria the following text, *''It aims to cover all different kinds of IT products and systems and presents a broad spectrum of requirements, leaving the product or system developer the task of defining the scope, called Target of Evaluation (TOE) and the selection of the set of requirements that apply for that specific case.* However, there is no text in Clause 5.4 which links 'Common criteria' or TOE to ensuring the data integrity and protection of PHIs in the ICTs of any organization providing a health service	TC211 is requested to consider ensuring that the next version for this document contains a direct link between the application of the TOE concept to PHI (and change the proposed definitions accordingly).	
SC 32-54	Clause 3.57	testing	te	The focus of any testing in a privacy protection context should be the data or PHI. The NOTE seems to exclude ''data''. This means that the object of conformance should be the HER, and the PHI which it contains.	Advice TC 211 to amend the current proposed term & definition to read as follows:	

				Also ‘’testing’’ is a generic concept. TS 14441 would benefit from placing it in a privacy protection context and focus, i.e. ‘privacy testing’’	**3.52** **privacy testing** determination of one or more characteristics of the **PHI** in an **EHR** and its associated ICT system, as the object of a defined conformity assessment, according to a pre-defined procedure which supports applicable privacy protection requirements	
SC 32-55	Clause 3.58	third-party conformity assess-ment activity	te	See comments on Clauses 3.17 and 3.51 above	Resolve in the same manner as for Clause 3.17 & 3.51.	
SC 32-56	Clause 3.59	threat	te	The focus of TS 14441 that of privacy requirements and thus any ‘’threat” would be to the individual and in particular the ‘’personal health information’’(PHI) of that individual Therefore one should consider focussing here on ‘’privacy threat’’	Amend and focus ‘threat’ on privacy and in the context of threat to personal information. Here is some draft text **privacy threat** potential cause of an unwanted incident or action with respect to **personal health information (PHI)**, which may result in harm to the **individual** or the **organization** which hold such **PHI,** and as such may cause a breach of applicable privacy protection requirements by the **organization**	
SC	Clause	vulnerabi-	te	Comment similar in nature a that for Clause	Amend and focus ‘’vulnerability’’ on	

32-57	3.60	lity		3.59	‘’privacy vulnerability’’ and place in context of PHI. Here follows some draft text: **privacy vulnerability** weakness of an assets or control of a **health information system** that can be exploited by a **privacy threat**	

END