HL7 EHR Work Group

Personal Health Record System Functional Model, Release 1
Draft Standard for Trial Use
July 2008

Chapter Five: Information Infrastructure Functions

EHR Work Group co-chairs:

Donald T. Mon, PhD
American Health Information Management Association (AHIMA)

John Ritter

Corey Spears
Practice Partners – McKesson

Pat Van Dyke
The ODS Companies, Delta Dental Plans Association

HL7® PHR Standard, © 2008 Health Level Seven®, Inc. ALL RIGHTS RESERVED. The reproduction of this material in any form is strictly forbidden without the written permission of the publisher.

HL7 and Health Level Seven are registered trademarks of Health Level Seven, Inc. Reg. U.S. Pat & TM Off

Table of Contents

1 Example 2
2 Actors 2
3 The 'Manage Hierarchy' 2
4 PHR Account Holder Privacy 3
5 Functionality Versus Implementation 4
6 Functional Outline 4
IN.1 (Health Record Information Management) 5
IN.1.1 (Data Management) 6
IN.1.2 (Synchronization) 7
IN.1.3 (Present Ad-Hoc Views of the Health Record) 8
IN.1.4 (Extraction of Health Record Information) 8
IN.1.5 (Store and Manage Unstructured Health Record Information) 10
IN.1.6 (Store and Manage Structured Health Record Information) 11
IN.1.7 (Patient Locator and Directory Services) 11
IN.1.8 (Standard Terminologies and Terminology Models) 12
IN.1.9 (Maintenance and Versioning of Standard Terminologies) 13
IN.1.10 (Terminology Mapping) 14
IN.1.11 (Administrative Management of Business Rules) 15
IN.1.12 (Workflow Management) 17
IN.2 (Standards Based Interoperability) 17
IN.2.1 (Interoperability Standards) 18
IN.2.2 (Interoperability Standards Versioning and Maintenance) 20
IN.2.3 (Standards Based Application Integration) 23
IN.2.4 (Interoperability Agreements) 23
IN.3 (Security) 24
IN.3.1 (Entity Authentication) 25
IN.3.2 (Entity Authorization) 27
IN.3.3 (Entity Access Control) 28
IN.3.4 (Non-Repudiation) 29
IN.3.5 (Secure Data Exchange) 30
IN.3.6 (Secure Data Routing) 31
IN.3.7 (Information Attestation) 32
IN.3.8 (Patient Privacy and Confidentiality) 33
IN.3.9 (Service Availability) 35
IN.3.10 (Secure Messaging) 35
IN.4 (Auditable Records) 36

Copyright © 2008 HL7, All Rights Reserved

Chapter 5: Information Infrastructure PHR-S Functions

Information Infrastructure PHR-S functions are the subset of PHR-S functions that support the Personal Health and Supportive functions. Information Infrastructure functions ensure that the PHR-S provides information privacy and security, promotes interoperability between PHR (and potentially, EHR) systems, and help make PHR features accessible and easy to use. Information Infrastructure functions may be provided by the applications that support managing the health record, supporting infrastructure or a combination of both.

1 Example

Since Personal Health and Supportive PHR-S functions must operate in a secure environment, Information Infrastructure functions ensure that PHR data (such as an immunization record) can only be viewed and updated after an individual or system authenticates with the PHR-S. For example, to open the PHR-S application and view an immunization record, a person may enter a User ID and password on a Web portal page. The application verifies that the security credentials are correct and then presents the immunization record page for that person using Secure Socket Layer encryption. If the person then elects to enter information about a flu shot received at a community clinic, the information may be selected from a drop-down list of common immunizations. After confirming that the information is correct, the PHR-S then contacts EHR systems with which the person has elected to share information. The PHR-S authenticates itself to the receiving system and requests authentication credentials from the EHR-S. Once credentials are confirmed, a secure data channel is created and the appropriate EHR information is transferred to the EHR-S; the immunization information contains metadata that show it is self-reported information. Finally, an audit log is created that shows what information was transferred to the EHR-S along with a date and time stamp that details when the transfer occurred.

2 Actors

Information Infrastructure functions are expected to be performed transparently by PHR-S applications on behalf of PHR-S end-users. A PHR-S may be “tethered” to an EHR-S, or may be a stand-alone system. A PHR-S may be sponsored and hosted by an organization, or may come as “shrink-wrapped” software to be deployed on an individual’s computer. Thus, the role of a System Administrator may be continual (i.e., involved in all ongoing operations related to configuring and managing the PHR-S), or the System Administrator may only set initial operational parameters for the PHR-S with no ongoing responsibility. In a similar way, a Security Administrator may be responsible only for reviewing the initial security controls for compliance with these criteria rather than having an ongoing role.

3 The “Manage Hierarchy”

Within the PHR Work Group, there was an intentional effort to create language consistency in the conformance criteria. The “Manage Hierarchy” diagram below was used to create semantic harmony within the conformance criteria so that, for example, if the Personal Health Chapter has a conformance criteria using the term “nullify”, that term had the same meaning as used in the Supportive Chapter’s conformance criteria.

Copyright © 2008 HL7, All Rights Reserved

The levels in the hierarchy are granular and have a parent-child relationship. For example, the diagram below depicts that managing the "Capture" of information comes from an External Source or from an Internal Source. Similarly, under the "Maintain" section of the diagram, the term "Store" could invoke all five verbs listed below it (i.e., Save, Backup, Compact, Encrypt, or Archive). If the parent term is not used, then the respective verbs in the child will be cited individually in the criterion. If the term "Manage" is used, all of the applicable verbs included in the table are encompassed in that criterion. Authors are responsible for determining whether one or more of the subverbs are not appropriate for a given function and must write conformance criteria that constrain the use of the verb hierarchy according to the intent of the profile being created.

MANAGE							
Capture		**Maintain**				**Render**	
Input (External)	Create (Internal)	Store	Update	Restrict Access	Remove Access	Read (Internal)	Output (External)
Receive Accept Download Import	Enter Compute Record	Save Backup Compact Encrypt Archive	Edit Correct Amend Augment Annotate Comment Associate Tag	Hide Mask Filter	Obsolete Inactivate Destroy Nullify Purge	View Report Display Access Present	Send Upload Export Synchronize

The hierarchical principle above was applied during the development of the PHR-S FM. Additional terms used in the model are found in the model's Glossary. It is important to be consistent in the terminology used in the PHR-S FM conformance criteria so there is consistent interpretation of the conformance criteria's intent in defining the functionality.

4 PHR Account Holder Privacy

It is the bias of this model that consumer privacy rights be protected to the fullest extent possible. However, as an international model that attempts to describe functionality for many PHR system sub-types (e.g., integrated PHR/EHR systems, stand-alone PHR systems, or vendor-provided Web-based systems), statements concerning consumer control over information are frequently tempered by the phrase (with some variations) "in accordance with user role, organizational policy, or jurisdictional law." This phrase does not extend license to institutions to violate individual rights, but acknowledges that legitimate exceptions may exist to the general rule of PHR Account Holder control over PHR-S information. In all cases, the model requires that the privacy policy of a PHR system be fully transparent to PHR Account Holders, and that a PHR-S has the ability to capture a PHR Account Holder's consent on how his or her personal information may be used and disclosed (see functions in IN.3.8, Patient Privacy and Confidentiality for additional detail.)

Copyright © 2008 HL7, All Rights Reserved

5 Functionality Versus Implementation

It is important to note that many functions provide the capacity for functionality (e.g., provide for standards-based interoperability), but do not give implementation details. A function, when implemented, must be implemented within the context of the entire PHR-S FM. For example, implementation of many functions throughout the model are expected to conform to the security and audit functions found within IN.3 (Security) and IN.4 (Auditable Records), and functions performed "by the PHR Account Holder" may be actually performed by others as delegated by the PHR Account Holder (see IN.3.2, Entity Authorization).

6 Functional Outline – Information Infrastructure

Information Infrastructure	IN.1	Health Record Information Management
	IN.2	Standards Based Interoperability
	IN.3	Security
	IN.4	Auditable Records

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
IN.1	**H**	Health Record Information Management	**Statement**: Capture, store, secure, message, display and report PHR information across PHR-S applications. Help ensure information entered by or on behalf of a PHR Account Holder is accurate. Facilitate appropriate identity checks before linking or transferring information between PHR records. **Description**: Since PHR information will typically be available on a variety of PHR-S applications, a PHR-S must provide the ability to manage the information and help ensure that when information is entered in or transferred to the PHR-S, it is information that belongs within the PHR-S of the PHR Account Holder. Information stored within the PHR-S should retain its integrity. PHR information may be defined differently based on context, and a PHR-S must translate information so it is accurate when context changes (e.g., lab results defined according to one data standard can be translated to another standard and still accurately reflect the health status and needs of an individual). Audit capabilities must be provided for troubleshooting and for forensic/legal purposes. Over time, minimum data sets and taxonomies will emerge, and the PHR-S should take advantage of these to promote interoperability between PHRs and between PHRs and EHRs. **Examples**: Minimum data sets include those defined by: 1) national health systems; 2) payer organizations; 3) governments; and 4) standards development organizations. Examples of standard taxonomies include ICD-9, CPT-4 and SNOMED. Methods to ensure data integrity include data comparisons (e.g., gender, date of birth) before information transfer to confirm that PHR information belongs to an intended individual. Designing products supported by human factors testing can help users to enter PHR information accurately and with minimal confusion.	IN.2			1

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
IN.1.1	**F**	Data Management	**Statement:** Manage health record information according to user role and, as applicable, organizational policy, or jurisdictional law. **Description:** Managing health information includes: - retaining inbound documents in the format as originally received so they may be reconstructed as sent to the receiving PHR-S; - documenting the method (fax, scanned document, electronically transferred) in which data or a document was received into the PHR-S; - storing and retrieving information in a semantically intelligent and useful manner (e.g., chronologically); - defining and applying classifications (metatags) related to structured and unstructured data; - ensuring availability of information for the legally prescribed period of time to system users; and - providing the ability to destroy and/or remove access to PHR data/records in a systematic way (including the archiving of records) according to organizational policy or jurisdictional law.	IN.2.1		1. The PHR-S **SHALL** provide the ability to store and retrieve health record data, and clinical documents for the legally prescribed time as applicable.	2
						2. The PHR-S **SHALL** provide the ability to retain inbound data or documents (related to health records) in the format originally received (unaltered, inclusive of the method in which they were received) for the legally or organizationally prescribed time in accordance with users' role, organizational policy, or jurisdictional law.	3
						3. The PHR-S **SHALL** retain the content of inbound data (related to health records) as originally received for the legally prescribed time.	4
						4. The PHR-S **SHOULD** provide the ability to retrieve both the information and business context data within which that information was obtained.	5
						5. The PHR-S **SHOULD** provide the ability to retrieve all the elements included in a minimum data set.	6
						6. The PHR-S **MAY** provide the ability to identify specific PHR data/records for access removal and will allow user confirmation before it occurs, and implement function IN.4 (Auditable Records).	7
						7. IF the PHR-S provides the ability to identify specific PHR data/records for access removal, THEN the PHR-S **SHALL** allow PHR Account Holder confirmation before it occurs, and implement function IN.4 (Auditable Records).	8
						8. The PHR-S **SHOULD** provide the ability to destroy PHR data/records so that all traces are irrecoverably removed in accordance with organizational policy and jurisdictional law.	9

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
						9. The PHR-S **SHOULD** pass record retention information (if any) when providing records to another entity.	10
						10. The PHR-S **MAY** provide an archive function or archiving mechanism for the authorized user to store records.	11
						11. The PHR-S **SHALL** permit the PHR Account Holder to define PHR information as private, and restrict views of such data in implementing IN.1.3 (Present Ad-Hoc Views of the Health Record) and IN.3.2 (Entity Authorization).	12
						12. The PHR-S **MAY** permit the PHR Account Holder to define and apply a classification scheme to structured and unstructured data.	13
IN.1.2	**F**	Synchronization	**Statement:** Maintain synchronization involving: - Interaction with entity directories; - Linkage of received data with existing entity records; - Location of each PHR component; and - Communication of changes between key systems. **Description:** A PHR-S may consist of a set of components or applications; each application manages a subset of the PHR information. Therefore it is important that, through various interoperability mechanisms, a PHR-S maintains all the relevant information regarding the PHR in synchrony. **Example**: If a PHR Account Holder has received a Magnetic Resonance Image (MRI) procedure, the system should be able to link the MRI image, a summary of results, and information about the referring physician. The late arriving MRI report should be linked to the original event in a seamless manner in order to provide a complete description of the MRI event.	IN.2.3		1. The PHR-S **SHALL** conform to function IN.2.1 (Interoperability Standards).	14
						2. The PHR-S **SHOULD** conform to function IN.1.7 (Patient Locator and Directory Services) to enable the use of registries and directories.	15
						3. The PHR-S **SHOULD** provide the ability to link entities to external information.	16
						4. The PHR-S **SHOULD** store the location of each known health record component in order to enable authorized access to a complete logical health record if the PHR is distributed among several applications within the PHR-S.	17

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
IN.1.3	**F**	Present Ad Hoc Views of the Health Record	**Statement:** Present ad hoc views of the PHR information, in accordance with user roles, organizational policies and jurisdictional laws as related to privacy and confidentiality. **Description:** The customized views and/or summarized information will enable an authorized user to find information that is important and/or meaningful to him or her, easily and in an organized manner. This function must perform such that only information that the user has been authorized to view can be seen in any ad-hoc view. **Examples:** Options to locate specific information in the PHR include keyword searches and sorting menus according to various categories of data.	-S		1. The PHR-S **SHOULD** provide the ability for an authorized user to create customized views of summarized information based on sort and filter controls for date or data range, problem, or other clinical data element or categories (e.g., medications, providers, or diagnoses).	18
						2. The PHR-S **SHOULD** provide the ability to access summarized information through customized views based on prioritization of chronology, problem, or other pertinent information of importance to the PHR Account Holder.	19
						3. The PHR-S **SHALL** conform to function IN.3.2 (Entity Authorization).	20
						4. The PHR-S **SHALL** conform to function IN.3.3 (Entity Access Control).	21
						5. The PHR-S **SHALL** conform to function IN.4 (Auditable Records).	22
IN.1.4		Extraction of Health Record Information	**Statement:** Provide data extraction capabilities, including data aggregation, in accordance with data exchange, analysis, reporting and printing requirements as authorized by the PHR Account Holder. **Description:** Extracted data may require use of more than one application and it may be pre-processed (for example, by being de-identified) before transmission. Data extractions may be used to exchange data and provide reports for primary and ancillary purposes. A PHR-S enables an authorized user to access and aggregate the distributed information, which corresponds to the health record or records that are needed for viewing, reporting, disclosure, etc. A PHR-S should support data extraction operations across the complete data set that constitutes the health record of an individual and provide an output that fully chronicles that individual's healthcare experience. Data extractions are used as input to patient care coordination between facilities, organizations and settings. In addition, data extractions can be used for administrative, financial, research, quality analysis, and public health purposes.	IN.2.4		1. The PHR-S **SHALL** provide the ability to extract health record information.	23
						2. The PHR-S **SHALL** conform to function IN.3.5 (Secure Data Exchange) to provide secure data exchange capabilities.	24
						3. The PHR-S **SHOULD** provide the ability to de-identify extracted information.	25
						4. The PHR-S **SHOULD** conform to function IN.2.1 (Interoperability Standards) to enable data extraction in standards-based formats.	26
						5. The PHR-S **SHOULD** provide the ability to perform extraction operations across the complete data set that constitutes the health record of an individual within the PHR-S.	27
						6. The PHR-S **SHOULD** provide the ability to perform extraction operations across a partial data set.	28

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			However, information should be extracted and used only in conformance with the privileges the PHR Account Holder has granted. These privileges may be defined by user status, acceptance of product terms and conditions, contractual information, organizational policies, and/or jurisdictional law. Data extraction can be to a variety of devices to promote transportability, such as a USB thumb drive, smart card or cellular phone. Data extraction can allow for the PHR Account Holder to print a copy of compiled records. The PHR-S should enable printing on paper which is easily obtained within the PHR Account Holder's home country (e.g., North American "letter" sized paper). "Printing" can also mean formatting the aggregated record in a universally-available format (such as a PDF) which can be electronically stored in a format compatible with the paper type locally used, and subsequently printed on paper at a later date. Note that the PHR-S has no obligation to provide supplies (paper, ink, etc.) for such printing. **Examples:** The printed PHR may be used during an appointment with a provider who has not yet been authorized to access the electronic PHR or who does not have electronic capabilities. A PHR Account Holder may print out a copy of key aggregated PHR information in anticipation of a natural disaster which might prevent electronic access. A proxy user who has been authorized to see a limited view of a PHR record may print out a version of the record that reflects their authorized view of the PHR data.			7. The PHR-S **SHOULD** provide the ability to perform extraction operations whose output fully chronicles the healthcare process.	29
						8. The PHR-S **SHOULD** provide the ability to extract data for administrative purposes as authorized by the PHR Account Holder.	30
						9. The PHR-S **SHOULD** provide the ability to extract data for financial purposes as authorized by the PHR Account Holder.	31
						10. The PHR-S **SHOULD** provide the ability to extract data for research purposes as authorized by the PHR Account Holder.	32
						11. The PHR-S **SHOULD** provide the ability to extract data for quality analysis purposes as authorized by the PHR Account Holder.	33
						12. The PHR-S **SHOULD** provide the ability to extract data for public health purposes as authorized by the PHR Account Holder.	34
						13. The PHR-S **SHALL** provide the ability for the PHR Account Holder or designee to print PHR information in a format compatible with a common/standard piece of paper.	35
IN.1.5	**F**	Store and Manage Unstructured Health Record Information	**Statement:** Store and manage select health record information as unstructured data. **Description**: Unstructured health record information is information that is not divided into discrete fields AND not represented as numeric, enumerated or codified data. Managing healthcare data includes capture, retrieval, deletion, correction, amendment, and augmentation. Augmentation refers to providing additional information regarding the healthcare data, which is not part of the data itself (e.g., linking patient consents or authorizations to the	IN.2.5.1		1. The PHR-S **SHALL** capture unstructured health record information.	36
						2. The PHR-S **SHALL** retrieve unstructured health record information.	37
						3. The PHR-S **SHALL** provide the ability to append unstructured health record information to existing PHR information.	38
						4. The PHR-S **SHALL** conform to function IN.1.1 (Data Management).	39

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			healthcare data of the patient). **Examples:** Unstructured health record information includes text, images, and multimedia. Specific examples may include a text message to physician, patient photo, or a scanned image of an insurance card.			5. The PHR-S **SHOULD** provide the ability to report unstructured health record information.	40
						6. The PHR-S **SHALL** provide the ability to append health record information to the original unstructured health record information. A specific type of implementation is not implied.	41
IN.1.6	**F**	Store and Manage Structured Health Record Information	**Statement:** Store and manage select health record information as structured data. **Description**: Structured health record information is information that is divided into discrete fields and is typically represented as numeric, enumerated or codified data. Managing healthcare data includes capture retrieval, deletion, correction, amendment, and augmentation. Augmentation refers to providing additional information regarding the healthcare data, which is not part of the data itself, e.g., linking patient consents or authorizations to the healthcare data of the patient. **Examples**: Structured health information include, a patient address, diastolic blood pressure, coded diagnosis, and a patient risk assessment questionnaire with multiple-choice answers	IN.2.5.1		1. The PHR-S **SHALL** capture structured health record information.	42
						2. The PHR-S **SHALL** retrieve structured health record information.	43
						3. The PHR-S **SHALL** provide the ability to append structured health record information to existing PHR information.	44
						4. The PHR-S **SHALL** conform to function IN.1.1 (Data Management).	45
						5. The PHR-S **SHOULD** provide the ability to report structured health record information.	46
						6. The PHR-S **MAY** track structured health record information over time.	47
						7. The PHR-S **SHOULD** provide the ability to retrieve each item of structured health record information discretely.	48
						8. The PHR-S **SHALL** provide the ability to append health record information to the original structured health record information. A specific type of implementation is not implied.	49
IN.1.7	**F**	Patient Record Locator and Directory Services	**Statement**: With the consent of the PHR Account Holder, or as affirmatively required by law, enable the use of patient record locator services and directories to uniquely identify, locate and supply links for retrieval of information related to: - patients and providers for healthcare purposes; - payers, health plans, sponsors, and employers for administrative and financial purposes; - public health agencies for healthcare purposes; and - related systems and devices for resource management purposes.	IN.3		1. The PHR-S **SHALL** provide the ability to use patient record locator services and directories.	50
						2. The PHR-S **SHALL** provide the ability to securely use patient record locator services and directories.	51
						3. The PHR-S **SHALL** conform to function IN.2.1 (Interoperability Standards) to provide standard data interoperability capabilities for using patient record locator services and directories.	52

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Description: Patient locator and directory service functions are critical to successfully managing the security, interoperability, and the consistency of the health record data across a PHR-S. These services enable the linking of relevant information across multiple information sources within, or external to, a PHR-S for use within an application. Directories and patient record locator services support communication between PHR systems, and other complementary systems and devices, and may be organized hierarchically or in a federated fashion. **Example:** A local directory usage is a PHR-S application broadcasting a patient's new phone number to providers and systems maintaining demographic information about that patient. Alternately, a service may automatically route new immunization information to a school administrator. In the future, a patient may be able to subscribe to a service which can uniquely identify the patient to various service organizations, facilitating identity management among healthcare providers and systems.			4. The PHR-S **SHOULD** communicate with local patient record locator and directory services through standardized interfaces.	53
						5. The PHR-S **SHOULD** communicate with non-local patient record locator and directory services (that is, to services that are external to PHR-S) through standardized interfaces.	54
						6. The PHR-S **SHOULD** provide the ability to use patient record locator services or directories with the consent of the PHR Account Holder or as affirmatively required by law to uniquely identify patients.	55
						7. The PHR-S **SHOULD** provide the ability to use directories to uniquely identify providers.	56
						8. The PHR-S **MAY** provide the ability to use patient record locator services or directories to retrieve links to relevant healthcare information regarding a patient.	57
						9. The PHR-S **MAY** provide the ability to use patient record locator services and directories to supply links to relevant healthcare information regarding a patient.	58
						10. The PHR-S **MAY** provide the ability to use directories to identify payers, health plans, and sponsors for administrative and financial purposes.	59
						11. The PHR-S **MAY** provide the ability to use directories to identify employers for administrative and financial purposes.	60
						12. The PHR-S **MAY** provide the ability to use directories to identify public health agencies for healthcare purposes.	61
						13. The PHR-S **MAY** provide the ability to use directories to identify healthcare related systems and devices for resource management purposes.	62
IN.1.8	**F**	Standard Terminologies and Terminology Models	**Statement:** Employ standard terminologies to ensure data correctness and to enable semantic interoperability (both within an enterprise and externally). Support a formal standard terminology model.	IN.4.1		1. The PHR-S **SHALL** provide the ability to use standard terminologies and terminology models to communicate with other PHR systems (internal or external to the PHR-S).	63

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Description: Semantic interoperability requires standard terminologies combined with a formal information model. A terminology provides semantic and computable identity to its concepts. Terminologies are use-case dependent and may be realm dependent. Formal standard terminology models enable common semantic representations by describing relationships that exist between concepts within a terminology or in different terminologies. The clinical use of standard terminologies is greatly enhanced with the ability to perform hierarchical inference searches across coded concepts. Relationships between concepts in a terminology are used in the search to recognize child concepts of a common parent. Clinical and other terminologies may be provided through a terminology service internal or external to a PHR-S. **Examples:** An example of a terminology service is described in the HL7 Common Terminology Services specification. An example of an information model is the HL7 Reference Information model. LOINC, SNOMED, ICD-9, ICD-10, and CPT-4 are examples of formal standard terminology models. Some models may be more applicable in certain contexts (physician review of diagnoses vs. consumer view of diagnoses). In using hierarchical information, a parent concept such as, "penicillin containing preparations" can have numerous child concepts, each of which represents a preparation containing a specific form of penicillin.			2. The PHR-S **SHALL** provide the ability to validate that clinical terms and coded clinical data exists in a current standard terminology.	64
						3. The PHR-S **SHOULD** provide the ability to exchange healthcare data using formal standard information models and standard terminologies.	65
						4. The PHR-S **SHOULD** provide the ability to use a formal standard terminology model.	66
						5. The PHR-S **SHOULD** provide the ability to use hierarchical inference searches (e.g., subsumption across coded terminology concepts that were expressed using standard terminology models).	67
						6. The PHR-S **SHOULD** provide the ability to use a terminology service (internal or external to the PHR-S).	68
						7. IF there is no standard terminology model available, THEN the PHR-S **MAY** provide a formal explicit terminology model.	69
						8. The PHR-S **SHALL** provide a means of allowing the PHR Account Holder to enter information into structured data formats using standard controlled clinical terminologies without the PHR Account Holder having to have any knowledge of the standards or specifications used.	70
						9. The PHR-S **SHALL** use text forms that do not include cryptic or uncommon abbreviations.	71
						10. The PHR-S **SHOULD** provide the ability to translate standard terminology into a vocabulary which is appropriate for the PHR Account Holder.	72
IN.1.9	**F**	Maintenance and Versioning of Standard Terminologies	**Statement:** Enable version control of standard terminologies according to customized policies to ensure maintenance of utilized standards. This version control includes the ability to accommodate changes to terminology sets as the source terminology undergoes its natural update process (i.e., new codes,	IN.4.2		1. The PHR-S **SHALL** provide the ability to use different versions of terminology standards.	73
						2. The PHR-S **SHALL** provide the ability to update terminology standards.	74

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			retired codes, or redirected codes). Such changes need to be cascaded to clinical content embedded in templates, custom formularies, etc., as determined by local policy. **Description:** Version control allows for multiple sets or versions of the same terminology to exist and be distinctly recognized over time. Terminology standards are usually periodically updated and concurrent use of different versions may be required. Since the meaning of a concept can change over time, it is important that retrospective review maintains the ability to relate changing conceptual meanings. If the terminology encoding for a concept changes over time, it is also important that retrospective analysis and research can correlate the different encodings to ensure the permanence of the concept. This does not necessarily imply that complete older versions of the terminology be kept in the PHR-S, only access to the changes needs to be maintained. It should be possible to retire deprecated versions when applicable business cycles are completed while maintaining obsolescent code sets.			3. The PHR-S **MAY** relate modified concepts in the different versions of a terminology standard to allow preservation of interpretations over time.	75
						4. The PHR-S **SHOULD** provide the ability to interoperate with PHR systems that use known different versions of a terminology standard.	76
						5. The PHR-S **SHOULD** provide the ability to retire and replace terminologies.	77
						6. The PHR-S **MAY** provide the ability to retire and replace individual codes within a terminology.	78
						7. The PHR-S **SHALL** provide the ability to cascade terminology changes where coded terminology content is embedded in clinical models (for example, templates and custom formularies) when the cascaded terminology changes can be accomplished unambiguously.	79
						8. Changes in terminology **SHALL** be applied to all new clinical content (via templates, custom formularies, etc.).	80
IN.1.10	**F**	Terminology Mapping	**Statement:** Map or translate one terminology to another as needed by local, regional, national, or international interoperability requirements **Description:** The ability to map or translate one terminology to another is fundamental to an organization in an environment where several terminologies are in play with overlapping concepts.	IN.4.3		1. The PHR-S **SHALL** provide the ability to use a terminology map.	81
						2. The PHR-S **SHOULD** provide the ability to use standard terminology services for the purposes of mapping terminologies.	82
						3. The PHR-S **MAY** provide the ability for an administrative user to validate a mapping.	83

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			It is a common occurrence that data is captured using one terminology, but is shared using another terminology. Realm specific (including local, regional, national or international) interoperability requirements can also determine the need for terminology mapping, and in many cases terminology mapping services can be used to satisfy these requirements. **Example:** There may be a need to map overlapping terminology concepts (e.g., between a PHR-S and an external laboratory system, or between a PHR-S and a billing system).			4. The PHR-S **MAY** provide the ability to create a terminology map.	84
IN.1.11	**F**	Administrative Management of Business Rules	**Statement:** Provide the ability to capture, maintain, and version-control the business rules. Apply business rules from necessary points within a PHR-S to control system behavior. A PHR-S audits the changes made to business rules, as well as changes to compliance to - and overrides of - applied business rules. **Description:** PHR-S business rule implementation functions include: decision support, workflow control, and access roles, as well as system and PHR Account Holder defaults and preferences. A PHR-S supports the ability of its creators to customize decision support components such as triggers, rules, or algorithms, as well as the wording of alerts and advice to meet realm specific requirements and preferences. The PHR-S may come with pre-defined business rules. However, these rules should be open to modification by the PHR Account Holder to meet specific needs. **Examples:** Examples of applied business rules include: - Flagging a combination of health behaviors as high-risk and providing appropriate guidance to the PHR Account Holder; - Sending an update to an immunization registry when a vaccination is administered; - Alerting a PHR Account Holder to competitive price information regarding medications; - Alerting a PHR Account Holder when PHR information is	IN.6		1. The PHR-S **SHALL** provide the ability to manage business rules.	85
						2. The PHR-S **SHOULD** provide the ability to create import, or access decision support rules to guide PHR-S behavior.	86
						3. The PHR-S **SHOULD** provide the ability to update decision support rules.	87
						4. The PHR-S **SHOULD** provide the ability to customize decision support rules and their components.	88
						5. The PHR-S **SHOULD** provide the ability to inactivate, obsolete, or destroy decision support rules.	89
						6. The PHR-S **SHOULD** conform to function IN.4 (Auditable Records) to audit all changes to decision support rules.	90
						7. The PHR-S **SHOULD** provide the ability to remove access to decision support rules.	91
						8. The PHR-S **SHOULD** conform to function IN.4 (Auditable Records) to audit all changes to diagnostic support rules.	92
						9. The PHR-S **SHOULD** provide the ability to create workflow control rules to guide PHR-S behavior.	93
						10. The PHR-S **SHOULD** provide the ability to update workflow control rules.	94

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			accessed (or access is attempted): a PHR Account Holder may modify this alert so that notification is only given when access is by someone not included in the Account Holder's provider list; - Alerting a proxy user when care may need to be provided to a dependent; - Limiting access to mental health information to only those permitted by the PHR Account Holder. Note: the PHR Account Holder may change who has access to this information at any time; - Preventing access to information to proxy users as directed by the PHR Account Holder; - Establishing system level defaults such as for vocabulary data sets to be implemented.; and - Establishing user level preferences such as allowing the use of health information for research purposes.			11. The PHR-S **MAY** provide the ability to customize workflow control rules and their components.	95
						12. The PHR-S **SHOULD** provide the ability to remove access to workflow control rules.	96
						13. The PHR-S **SHOULD** conform to function IN.4 (Auditable Records) to audit all changes to workflow control rules.	97
						14. The PHR-S **SHOULD** provide the ability to create access privilege rules and roles to guide PHR-S behavior.	98
						15. The PHR-S **SHALL** provide the ability to update access privilege rules.	99
						16. The PHR-S **SHALL** provide the ability to customize access privilege rules and their components.	100
						17. The PHR-S **MAY** provide the ability to inactivate, obsolete, or destroy access privilege rules.	101
						18. The PHR-S **MAY** conform to function IN.4 (Auditable Records) to audit all changes to access privilege rules.	102
						19. The PHR-S **SHOULD** conform to function IN.4 (Auditable Records) to audit all changes to other business rules.	103
						20. The PHR-S **SHOULD** support the ability to selectively export business rules.	104
						21. The PHR-S **SHOULD** support the ability to selectively import business rules.	105
IN.1.12	**F**	Workflow Management	**Statement:** Support workflow management functions related to business rules to direct the flow of end user tasks. **Description:** Workflow management functions that an PHR-S supports include: - Distribution of information to and from internal and external parties; - Support for task management as well as parallel and serial task distribution; and - Support for notification based on system triggers.	IN.7		1. The PHR-S **SHALL** employ measures to terminate idle sessions after a system specified, but configurable period of session inactivity.	106
						2. The PHR-S **SHOULD** use workflow-related business rules to direct the flow of work assignments.	107
						3. The PHR-S **SHOULD** provide the ability to create workflow (task list) queues.	108

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Workflow definitions and management may be implemented by a designated application or distributed across a PHR-S. **Examples:** A workflow may send an alert to an adult caregiver for an elderly patient, and that patient's personal care physician (PCP) when an alert had been sent to refill a prescription and the prescription had not been filled within a week. A patient decides to take St. John's Wort. When this information is entered into the PHR-S, an on-screen alert displays saying this herbal remedy may negatively interact with other medications the patient is currently taking.			4. The PHR-S **SHOULD** provide the ability to manage workflow (task list) queues.	109
						5. The PHR-S **MAY** use PHR-S interfaces that support the management of workflow (task lists) queues.	110
						6. The PHR-S **MAY** provide the ability to distribute information to and from internal and external parties.	111
						7. The PHR-S **MAY** provide the ability to route notifications and tasks based on PHR-S triggers.	112
						8. The PHR-S **MAY** dynamically escalate workflow according to business rules.	113
						9. The PHR-S **MAY** dynamically redirect workflow according to business rules.	114
						10. The PHR-S **MAY** dynamically reassign workflow according to business rules.	115
IN.2	**H**	Standards Based Interoperability	**Statement:** With the consent of the PHR Account Holder or as affirmatively required by jurisdictional law, provide automated health care delivery processes and seamless exchange of clinical, administrative, and financial information through standards-based solutions. **Description:** Interoperability standards enable a PHR-S to operate as a set of applications. This results in a unified view of the system where the reality is that several disparate systems may be coming together. **Examples:** Interoperability standards can enable the sharing of information between different PHR systems, between PHR and EHR systems, and between PHR systems and public health systems, payer/health plan systems, and pharmacy systems. Interoperability standards allow for the timely and efficient access to and capture of information with minimal impact to the PHR Account Holder.	IN.5			116
IN.2.1	**F**	Interoperability Standards	**Statement:** Support the ability to operate seamlessly with other systems, either internal or external, that adhere to recognized interoperability, security and privacy standards.	IN.5.1		1. The PHR-S **SHALL** provide the ability to use interoperability standards as required by realm specific and/or local profiles.	117

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			"Other systems" include other PHR and EHR Systems, applications within a PHR-S, or other authorized entities that interact with a PHR-S. **Description:** The PHR-S typically uses a number of interoperability standards to meet its external and internal interoperability requirements, and there must be a common understanding of rules regarding connectivity, information structures, formats and semantics. These are known as interoperability or interchange standards. Data exchange which may be between internal systems or modules, or external to the PHR-S, is to occur in a manner which is seamless to the PHR Account Holder. If interoperability involves double entry, or manual cut-and-paste steps by the user, it is not considered seamless. Representation of PHR content is transmitted in a variety of interoperability formats such as: HL7 Messages, Clinical Document Architecture (CDA) and other HL7 Structured Documents, X12N healthcare transactions, and Digital Imaging and Communication in Medicine (DICOM) format. Support for multiple interaction modes is needed to respond to differing levels of immediacy and types of exchange. For example, messaging is effective for many near-real time, asynchronous data exchange scenarios but may not be appropriate if the end-user is requesting an immediate response from a remote application. Standard terminology is a fundamental part of interoperability and a formal explicit information model further optimizes interoperability. Organizations typically need to deal with more than one information model and may need to develop a mapping or a meta-model. Delivery confirmation processes provide system assurance that an attempted interchange actually occurred. **Examples:** A variety of interaction modes are typically supported such as: - Unsolicited Notifications (e.g., the PHR Account Holder receives a notification from his/her healthcare team regarding a new development related to their condition). - Query/Response (e.g., "Show me the latest lab results for my child.").			2. The PHR-S **SHALL** provide the ability to seamlessly perform interoperability operations with other PHR systems or EHR systems that adhere to recognized interoperability standards.	118
						3. The PHR-S **SHALL** conform to function IN.1.8 (Standard Terminologies and Terminology Services) to support terminology standards in accordance with a user's role, organizational policy, or jurisdictional law.	119
						4. The PHR-S **SHOULD** provide the ability to exchange data using an explicit and formal information model and standard, coded terminology.	120
						5. IF there is no standard information model available, THEN the PHR-S **MAY** provide a formal explicit information model in order to support the ability to operate seamlessly with other systems.	121
						6. The PHR-S **SHOULD** have the ability to exchange its data content with other systems.	122
						7. The PHR-S **SHOULD** have the ability to synchronize a minimum data set with another system.	123
						8. The PHR-S **SHOULD** request delivery confirmation from a system external to the PHR-S whenever information is sent by the PHR-S to that system.	124
						9. The PHR-S **SHOULD** log and maintain a record of each delivery confirmation request that it sends to a system external to the PHR-S, and each delivery confirmation it receives in response.	125
						10. The PHR-S **SHOULD** provide confirmation to a system external to the PHR-S whenever that system requests confirmation that information it sent was accepted by the PHR-S.	126

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			- Service Request and Response (e.g., "Look up a recent episode of care and find out the number of patients a doctor sees for that condition, as well as the quality/cost estimates for that treatment."). - Information interoperability between my PHR (properly deidentified) and public health organizations; - Structured/discrete clinical documents (e.g., "Here is my updated list of allergies."). - Unstructured clinical document (e.g., "Add a free-text annotation in my diabetes diary as to how I feel today.").			11. The PHR-S **SHOULD** log and maintain a record of each delivery confirmation request it receives from a system external to the PHR-S, and each delivery confirmation it sends in response.	127

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
IN.2.2	**F**	Interoperability Standards Versioning and Maintenance	**Statement:** Enable version control according to local policies to ensure maintenance of utilized interoperability standards. **Description**: Version control of an interoperability standard implementation includes the ability to accommodate changes as the source interoperability standard undergoes its natural update process. The life cycle of any given standard results in changes to its requirements. It is critical that an organization know the version of any given standard that it uses and what it's requirements and capabilities are. Interoperability standards that are backward compatible support exchange among senders and receivers who are using different versions. Version control ensures that those sending information in a later version of a standard consider the difference in information content that can Interoperate effectively with receivers, who are capable of processing only earlier versions. That is, senders need to be aware of the information that receivers are unable to capture and adjust their business processes accordingly. **Examples:** [In the following examples, the term "organization" is synonymous with a collection of interoperating systems – i.e., the PHR-S and entities with which it engages in electronic data exchange (e.g., EHR-S, pharmacies, or public health systems).] If the organization migrates to an HL7 v2.5 messaging standard, it may choose to take advantage of new capabilities such as blood bank information. The organization may find that certain fields have been retained for backwards compatibility only or withdrawn altogether. Standards typically evolve in such a way as to protect backwards compatibility. However, sometimes there is little, or no, backwards compatibility when an organization may need to replace an entire standard with a new methodology (e.g., migrating from HL7 v2 to HL7 v3).	IN.5.2		1. The PHR-S **SHALL** provide the ability to use different versions of interoperability standards.	128

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Large (and/or federated) organizations typically need to use different versions of an interoperability standard to meet internal organizational interoperability requirements. For example, the enterprise-wide standard might use HL7 v2.5 for Lab messages, but some regions of the enterprise might be at a lower level. It should be possible to obsolete interoperability standards versions when applicable business cycles are completed while maintaining these versions. An example use of this is for possible claims adjustment throughout the claim's life cycle. When interoperability standards change over time, it is important that retrospective analysis and research correlate and note gaps between the different versions' information structures to support the permanence of concepts over time.			2. The PHR-S **SHALL** provide the ability to change (reconfigure) the way that data is transmitted as an interoperability standard evolves over time and in accordance with business needs.	129
						3. The PHR-S **SHOULD** provide the ability to retire and replace an interoperability standard.	130
						4. The PHR-S **SHOULD** provide the ability to interoperate with other PHR systems or EHR systems that use known earlier versions of an interoperability standard.	131
IN.2.3	**F**	Standards-Based Application Integration	**Statement:** Enable standards-based application integration. **Description:** When a PHR-S is based on a combination of applications, it must use standardized methods. Standards-based application integration may be achieved in a variety of ways. The method used depends on the organization's approach to application integration. An organization could conceivably use multiple integration approaches. **Examples:** - Context integration may be achieved via HL7 Clinical Context Object Workgroup (CCOW) standards; - User-based security and session integration may be achieved via Security Application Markup Language (SAML); - PHR-S may be integrated in an Enterprise Information System Architecture via Service Oriented Architecture (SOA) standards.	IN.5.3		1. The PHR-S **SHALL** provide the ability to support standards-based application integration when complemented by and/or composed of disparate applications.	132
IN.2.4	**F**	Interoperability Agreements	**Statement:** Support interactions with entity directories to determine the address, profile and data exchange requirements of known and/or potential partners.	IN.5.4		1. The PHR-S **SHOULD** use interoperability agreement descriptions when exchanging information with partners.	133

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Use the rules of interaction specified in the partner's interoperability agreement, including privacy and security requirements, when exchanging information. **Description:** Systems that wish to communicate with each other, must agree on the parameters associated with that information exchange. Interoperability Agreements allow a PHR-S to describe those parameters/criteria. A PHR-S can use the entity registries to determine the security, addressing, and reliability requirements between partners. A PHR-S can use this information to define how data will be exchanged between the sender and the receiver. Discovery of interoperability services and capabilities can be automatic, or alternately, an interoperability agreement may take the form of a requirements document which the interoperability partners agree to implement. **Examples:** - A new application can automatically determine a patient demographics source using a Universal Description and Discovery Integration (UDDI) for source discovery, and retrieve the Web Services Description Language (WSDL) specification for binding details; - Good Health Hospital is a member of AnyCounty LabNet, for sharing laboratory results with other partners. Good Health Hospital periodically queries LabNet's directory (UDDI) to determine if additional information providers have joined LabNet. When new information providers are discovered, the Good Health IT establishes the appropriate service connections based upon the Service Description (WSDL).			2. The PHR-S **SHOULD** use interoperability agreement description standards (when available).	134
						3. The PHR-S **MAY** conform to function IN.1.7 (Registry and Directory Services) to interact with entity directories to determine the address, profile and data exchange requirements of known and/or potential partners.	135
						4. The PHR-S **MAY** provide the ability to automatically discover interoperability services and capabilities.	136
IN.3	**H**	Security	**Statement:** Secure the access to a PHR-S and PHR information. Manage the sets of access control permissions granted within a PHR-S. Prevent unauthorized use of data, data loss, tampering and destruction. **Description:** To enforce security, all PHR-S applications must adhere to the rules established to control access and protect the privacy of PHR information. Security measures assist in preventing unauthorized use of data and protect against loss, tampering and destruction. A PHR-S must be	IN.1			137

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			capable of including or interfacing with standards-conformant security services to ensure that any Principal (user, organization, device, application, component, or object) accessing the system or its data is appropriately authenticated, authorized and audited in conformance with local and/or jurisdictional policies.				
IN.3.1	**F**	Entity Authentication	**Statement:** Authenticate PHR Account Holder and/or entities before allowing access to a PHR-S. **Description:** Both users and applications are subject to authentication. The PHR-S must provide mechanisms for users and applications to be authenticated. Users will have to be authenticated when they attempt to use the application, and the applications must authenticate themselves before accessing PHR information managed by other applications. Authentication typically occurs when a user (person or system) presents identity credentials, such as a User ID and password, which are validated against information held in a secure database. However, specifying particular methods of authentication to access a PHR-S are beyond the scope of this functional model. The method(s) selected by a PHR-S for authentication should be proportionate to the risk of granting inappropriate access to a PHR-S, and in fact may combine more than one method to provide additional identity assurance. In addition, how a PHR-S authenticates users should be subject to change over time as technologies and risks evolve. For the purposes of this model, we include methods of	IN.1.1		1. The PHR-S **SHALL** capture key demographic elements needed to uniquely identify the PHR Account Holder.	138
						2. The PHR-S **SHALL** verify the PHR Account Holder identity prior to granting access to information in the PHR.	139
						3. The PHR-S **SHALL** authenticate the PHR Account Holder prior to every session.	140
						4. The PHR-S **SHALL** authenticate authorized users other than the PHR Account Holder prior to every session.	141
						5. The PHR-S **SHALL** authenticate any other PHR systems, EHR systems or other related systems prior to any release of information about the PHR Account Holder.	142
						6. The PHR-S **SHALL** employ measures to prevent unauthorized access.	143
						7. The PHR-S **SHALL** prevent access to PHR-S applications or PHR-S data to all non-authenticated principals.	144
						8. The PHR-S **SHOULD** provide the ability to implement a Chain of Trust agreement.	145

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			extending access to other individuals which use a security token (e.g., knowledge of a shared secret or possession of a one-time pass code which is given to a user by the PHR Account Holder) as being valid methods for authentication (authentication is dependent on the presence of a valid security token). Chain of Trust relationships may be established that contractually state specific authentication mechanisms before data may be accessed or transferred to individuals and systems external to the PHR-S. The PHR-S may itself manage authentication credentials, or may rely on an external service to do so, in determining the validity of requests to create, read, update or transfer information residing in an individual's PHR. **Examples:** Note that the following list of authentication methods is not inclusive of all possible authentication methods but contains examples of typical authentication mechanisms currently in industry use. - username/password; - digital certificate; - secure token; - biometrics; - shared secret; - RFID tags linked to a known identity.			9. The PHR-S **MAY** provide the ability to manage authentication credentials to enable access and data exchange with systems external to the PHR-S.	146
IN.3.2	**F**	Entity Authorization	**Statement**: Manage the sets of access-control permissions granted to entities that use a PHR-S (PHR-S Users). Enable PHR Account Holders to extend partial or full access to PHR information to other individuals who can act on behalf of the PHR Account Holder (proxy users), clinicians, systems, and others. Enable PHR Account Holders to deny access to PHR information. Enable PHR Account Holders to determine what information may be accepted into a PHR Account Holder's PHR. **Description**: PHR-S users, other than the PHR Account	IN.1.2		1. The PHR-S **SHALL** allow the PHR Account Holder to assign different levels of access for Authorized Users.	147
						2. The PHR-S **SHALL** allow the PHR Account Holder to designate Proxy Users to access and conduct PHR-S functions on behalf of the PHR Account Holder.	148

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Holder, may be authorized to use the components of a PHR-S according to their identity, role and/or the patient's present condition. However, access may be typically extended on an explicit, individual basis (e.g., allowing a particular clinician access to all PHR information except for chemical dependency treatment notes). Note that these criteria are agnostic regarding the degree to which a PHR Account Holder may (or may not) be able to selectively import information from a given source and the granularity to which information may be masked/hidden before the PHR Account Holder shares portions of a PHR with others. At a minimum, the PHR Account Holder needs to: - say whether or not data as provided can be accepted into their PHR Account. In some instances this may mean that the user will decide to not import a document due to an objection over one piece of data provided within the document which cannot be "edited out". - know precisely what information would be available to an individual or entity before making an informed decision to share that information. **Examples:** User-based authorization refers to the permissions granted or denied based on the identity of an individual. An example of User-based authorization is a patient defined denial of access to all or part of a record to a particular party for privacy related reasons. A context-based example is a patient-granted authorization to a specific third party for a limited period to view specific PHR records. Another example is a right granted for a limited period to view those, and only those, PHR records connected to a specific topic of investigation. Examples of authorized users include school nurse, judicial system officers, insurance carriers, care providers, health program administrators/coaches, and secondary PHR users (e.g., public health, research organizations, and clinical trials).			3. The PHR-S **SHALL** provide a means for emergency access to clinical information which does not require action on the part of the PHR Account Holder to grant access. This access should always be in accordance with the directions of the PHR Account Holder.	149
						4. The PHR-S **SHALL** allow the PHR Account Holder to designate Authorized Users to access and conduct PHR-S functions.	150
						5. The PHR-S **SHOULD** provide the ability to allow PHR Account Holders discretion over the acceptance of information into their PHR systems.	151
						6. The PHR-S **SHALL** conform to function IN.4 (Auditable Records) for the purpose of recording all authorization actions.	152
						7. The PHR-S **MAY** permit access to previously unauthorized individuals in emergency situations and when legally-mandated.	153
IN.3.3	**F**	Entity Access Control	**Statement:** Verify and enforce access control to all PHR-S components, PHR information and functions for end-users, applications, sites, etc., to prevent unauthorized use of a resource.	IN.1.3		1. The PHR-S **SHALL** protect the security and privacy of PHR information.	154
						2. The PHR-S **SHALL** conform to function IN.3.1 (Entity Authentication).	155

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Description: Entity Access Control is a fundamental function of a PHR-S. To ensure that access is controlled, a PHR-S must perform authentication and authorization of users or applications for any operation that requires it and enforce the system and information access rules that have been defined.			3. The PHR-S **SHALL** conform to function IN.3.2 (Entity Authorization).	156
						4. The PHR-S **SHALL** provide the ability to define PHR-S and data access rules.	157
						5. The PHR-S **SHALL** enforce PHR-S and data access rules for all PHR-S resources (at component, application, or user level, either local or remote).	158
						6. The PHR-S **SHALL** provide the capability to prevent unauthorized use of the PHR-S data, services or functions.	159
IN.3.4	**F**	Non-Repudiation	**Statement:** Limit a PHR-S user's ability to deny (repudiate) the origination, receipt, or authorization of a data exchange by that user. **Description:** A PHR-S allows data entry and data access to a patient's personal health record. Non-repudiation guarantees that the source of the data record can not later deny that it is the source. Specifically, this means that the sender or receiver of a message cannot later deny having sent or received the message. **Examples:** Non-repudiation may be achieved through the use of: 1) a digital signature, which serves as a unique identifier for an individual (much like a written signature on a paper document); 2) confirmation service, which utilizes a message transfer agent to create a digital receipt (providing confirmation that a message was sent and/or received); and timestamp, which proves that a document existed at a certain date and time. Note: date and time stamping implies the ability to indicate the time zone where it was recorded (time zones are described in ISO 8601 Standard Time Reference).	IN.1.5		1. The PHR-S **SHALL** time stamp initial entry, modification, or exchange of data, and identify the actor/principal taking the action as required by organizational policy or jurisdictional law.	160
						2. The PHR-S **SHALL** provide additional non-repudiation functionality where required by organizational policy, or jurisdictional law.	161
						3. The PHR-S **SHALL** conform to function IN.4 (Auditable Records) to prevent repudiation of data origination, receipt, or access.	162
						4. The PHR-S **MAY** conform to function IN.3.7 (Information Attestation) to ensure the integrity of data exchange and thus prevent repudiation of data origination or receipt.	163
IN.3.5	**F**	Secure Data Exchange	**Statement:** PHR data needs to be exchanged securely. This requires measures to insure the confidentiality and integrity of the data. **Description:** Exchange of PHR information requires	IN.1.6		1. The PHR-S **SHALL** employ methods to assure integrity and privacy between the data source and intended destination, as well as provide means of assurance of receipt.	164

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			appropriate security and privacy considerations including data obfuscation and both destination and source authentication when necessary. For example, it might be necessary to encrypt data sent to remote destinations. This function requires that there is an overall coordination regarding what information is exchanged and how the exchange will occur, between PHR-S and entities with which it engages in electronic data interoperability. The policies applied at different locations must be consistent or compatible with each other in order to ensure that the information is protected when it crosses entity boundaries within the PHR-S or external to the PHR-S. Route electronically-exchanged PHR data only to/from known, registered, and authenticated destinations/sources (according to applicable healthcare-specific rules and relevant standards). **Examples:** Browser based interface uses SSL to view PHR; EHR-S to PHR-S uses x.509 certificate to identify EHR-S system to regional Identity Provider, and after authentication the regional Identity Provider provides a Security Assertion Markup Language (SAML) assertion defining the attributes of the EHR-S needed by the PHR-S to allow proper access and controls. For example, a common encryption algorithm for point-to-point transmission is 256-bit AES. An example encryption algorithm is 1024 RSA which is also used to effect digital signatures. Both of these are routinely used in generation of x.509 certificates. One example technology for securing the content of a message sent as a SOAP message would be Web Services Security (WSS) which permits encryption of specific elements, digital signatures as well as the permission information.			2. The PHR-S **SHALL** transmit any information about the PHR Account Holder in accordance with the directions of the PHR Account Holder.	165
						3. The PHR-S **SHALL** encrypt and decrypt PHR information that is exchanged over a non-secure link.	166
						4. The PHR-S **SHALL** include the PHR Account Holder's directions regarding subsequent release of PHR information.	167
						5. The PHR-S **SHALL** conform to function IN.3.6 (Secure Data Routing).	168
						6. The PHR-S **MAY** provide the ability to obfuscate data.	169
						7. The PHR-S **SHALL** support standards-based encryption mechanisms when encryption is used for secure data exchange.	170
IN.3.6	**F**	Secure Data Routing	**Statement:** Route electronically exchanged PHR data only to/from known, registered, and authenticated destinations/sources (according to applicable healthcare-specific rules and relevant standards).	IN.1.7		1. The PHR-S **SHALL** automatically route electronically exchanged PHR data only from and to authenticated sources and destinations and over secure networks.	171

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			Description: A PHR-S needs to ensure that it is exchanging PHR information with the entities (e.g., applications, institutions, directories) it expects. This function depends on entity authorization and authentication to be available in the system. For example, a system user may elect to send immunization records to a school admissions office. To accomplish this, the system must use a secure routing method, which ensures that both the sender and receiving sides are authorized to engage in the information exchange. Known sources and destinations can be established in a static setup or they can be dynamically determined. Examples of a static setup are recordings of IP addresses or recordings of DNS names. For dynamic determination of known sources and destinations systems can use authentication mechanisms as described in IN.1.1. (Data Management). For example, the sending of a lab result from a lab system to a PHR-S within the same organization usually uses a simple static setup for routing. In contrast sending a lab result to an institution outside of the organization will involve some kind of authentication process.			2. The PHR-S **MAY** route electronically exchanged PHR data to and from unauthenticated sources and destinations at the individual PHR Account Holder's direction.	172
						3. The PHR-S **SHOULD** conform to function IN.4 (Auditable Records) to provide audit information about additions and changes to the status of destinations and sources.	173
IN.3.7	**F**	Information Attestation	**Statement:** Manage electronic attestation of attestable information including the retention of the signature of attestation (or certificate of authenticity) associated with incoming or outgoing information. **Description:** The purpose of attestation is to show authorship and assign responsibility for an act, event, condition, opinion, or diagnosis. Every entry in the PHR must be identified with the author and should not be made or signed by someone other than the author. Attestable content may be received from related systems (e.g., EHR systems). Digital signatures may be used to implement document attestation. For an incoming document, the record of attestation is retained if included. Attestation functionality	IN.1.8		1. The PHR-S **SHALL** conform to function IN.3.1 (Entity Authentication).	174
						2. The PHR-S **SHALL** conform to function IN.3.2 (Entity Authorization).	175
						3. The PHR-S **SHALL** provide the ability to associate any attestable content added or changed to an PHR with the content's author (for example by conforming to function IN.4 (Auditable Records)).	176
						4. The PHR-S **SHALL** provide the ability for attestation of attestable PHR content by the content's author.	177
						5. The PHR-S **SHALL** indicate when attestable data has not been attested.	178

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			must meet applicable legal, regulatory or other standards or requirements. Attestation of PHR information promotes trustworthiness and use of PHR information by clinicians and other stakeholders. **Example:** An individual PHR Account Holder enters family history information into a PHR record. This information is shared electronically with a health care provider and, when entered into the provider's EHR system, the entry retains information that continues to attribute the history statements to the individual who provided them.			6. The PHR-S **MAY** provide the ability for attestation of PHR content by properly authenticated and authorized users different from the author as required by user role, organizational policy, or jurisdictional law.	179
						7. The PHR-S **MAY** provide the ability to use digital signatures as the means for attestation.	180
IN.3.8	**F**	Patient Privacy and Confidentiality	**Statement:** Enable the enforcement of the applicable jurisdictional and organizational patient privacy rules as they apply to various parts of a PHR-S through the implementation of security mechanisms. **Description:** Patients' privacy and the confidentiality of PHRs are violated if access to PHRs occurs without authorization anywhere PHR information exists (locally or over a distributed network). Violations or potential violations can impose tangible economic or social losses on affected patients, as well as less tangible feelings of vulnerability and pain. Fear of potential violations discourages patients from revealing sensitive personal information that may be relevant to diagnostic and treatment services. Rules for the protection of privacy and confidentiality may vary depending upon the vulnerability of patients and the sensitivity of records. Strongest protections should apply to the records of minors and the records of patients with stigmatized conditions. Authorization to access the most sensitive parts of a PHR is most definitive if made by the explicit and specific consent of the patient. Please see the definition of masking in the glossary. However, it must be noted that in many areas of the world, the legal status of a PHR record is undetermined. In	IN.1.9		1. The PHR-S **SHALL** provide the ability to fully comply with the requirements for patient privacy and confidentiality in accordance with organizational policy and jurisdictional law.	181
						2. The PHR-S **SHALL** provide the ability to maintain varying levels of confidentiality as specified by the PHR Account Holder and as required by jurisdictional law.	182
						3. The PHR-S **SHALL** provide the ability to manage PHR Account Holder consent to, or restrictions against, any use of data.	183
						4. The PHR-S **SHALL** conform to function IN.3.1 (Entity Authentication).	184
						5. The PHR-S **SHALL** conform to function IN.3.2 (Entity Authorization).	185
						6. The PHR-S **SHALL** conform to function IN.3.3 (Entity Access Control).	186
						7. The PHR-S **SHOULD** conform to function IN.3.4 (Non-Repudiation).	187
						8. The PHR-S **SHALL** conform to function IN.3.5 (Secure Data Exchange).	188
						9. The PHR-S **SHALL** conform to function IN.4 (Auditable Records).	189

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			addition, while these conformance criteria express a high normative standard for respecting patient privacy, PHR information is subject to legal discovery under certain circumstances.			10. The PHR-S **SHOULD** provide the ability to mask parts of the personal health record (e.g., medications, conditions, sensitive documents, ad-hoc views) from disclosure according to PHR Account Holder direction, user role, organizational policy or jurisdictional law.	190
						11. The PHR-S **SHOULD** provide the ability to override a mask in emergency or other specific situations as specified by the PHR Account Holder and as required by jurisdictional law.	191
						12. The PHR-S **SHALL** have a fully transparent privacy policy.	192
						13. The PHR-S **SHALL** provide the capability to capture PHR Account Holder consent to a fully transparent privacy policy.	193
						14. The PHR-S **SHALL** provide a means to capture authorized users' opt-in agreement to the terms and conditions of the PHR service.	194
IN.3.9	**F**	Service Availability	**Statement:** Availability refers to the days and hours a service is potentially ready for use. **Description:** The availability (days and hours of service for data access) and timeliness (response time to data requests) of the PHR-S should be specified in a Service Level Agreement (SLA) between the PHR Service Provider and the PHR Sponsor or PHR Account Holder. An SLA is important for a variety of reasons, including availability for emergency situations, and may help consumers determine which of many choices of PHR systems would best meet their needs and circumstances. We intend the implementation of this Function to be neutral as to the method it is fulfilled. For example, SLA information may be available at run-time, presented within a paper version of a Terms of Use agreement, or requested by phone. **Example:** A Service Level Agreement may state that the system is available 95% of the time, 7 days a week, 24 hours a day.			1. The PHR-S **SHALL** provide the ability for a user to obtain service level agreement information.	195
						2. The PHR-S **MAY** provide the ability for the PHR Account Holder to obtain performance statistics, including service availability statistics, as specified in the service level agreement.	196

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
IN.3.10	**F**	Secure Messaging	**Statement:** Enable secure electronic communication between PHR Account Holders and Health Care Providers. **Description:** A PHR Account Holder may send and receive electronic communication to and from an interested, capable provider in such a manner that identities are verified and information exchanges are encrypted during transmittal. **Example:** A PHR Account Holder composes a message to a health care provider asking for clarification about a treatment plan. Using functionality within the PHR-S, the PHR Account Holder's message is encrypted before being sent over the Internet, and the message contains information verifying the identity of the sender. The message recipient receives a "tickler" message through general e-mail which states the recipient has received a secure message from the PHR-S. The recipient authenticates identity to the PHR-S, and is then able to retrieve the secure message.			1. The PHR-S **SHOULD** provide the capability for PHR Account Holders and Health Care Providers to electronically communicate in a secure manner.	197
						2. The PHR-S **SHOULD** provide the ability to archive messages in the PHR-S.	198
IN.4	**F**	Auditable Records	**Statement:** Provide audit capabilities for system access and usage indicating who accessed the record, when, what actions were taken, and when the actions occurred. Examples of auditable actions include: created, modified, viewed, extracted or deleted a record. Date and time stamps require corresponding time zones (see ISO 8601 Standard Time Reference) and consistent time synchronization across complementary information systems (see IETS RFC 1305). Auditable records extend to information exchange, to audit of consent status management and to entity authentication attempts. Audit functionality includes the ability to generate audit reports and to interactively view change history for individual health records. Audit log formats may conform to standards such as IETS RFC 3881 (Security Audit & Access Accountability Message XML Data Definitions for Healthcare Applications). **Description:** Audit functionality extends to security audits, data audits, audits of data exchange, and the ability to generate audit reports. Audit capability settings should be configurable to meet the needs of local policies. PHR-S audit operations and policies should have two points of view.	IN.2.2		1. The PHR-S **SHALL** log access and usage of system, data, and organizational resources to minimally include who performed the action, what the action was, and when it was performed.	199
						2. The PHR-S **SHALL** conform to function IN.3.1 (Entity Authentication).	200
						3. The PHR-S **SHALL** audit access to PHR-S according to user role, organizational policy, or jurisdictional law.	201
						4. The PHR-S **SHALL** audit object or data creation according to user role, organizational policy, or jurisdictional law.	202
						5. The PHR-S **SHALL** audit object or data modification according to user role, organizational policy, or jurisdictional law.	203
						6. The PHR-S **SHALL** audit data extraction according to user role, organizational policy, or jurisdictional law.	204
						7. The PHR-S **SHALL** audit data exchange according to user role, organizational policy, or jurisdictional law.	205

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
			First, audit capabilities need to be present to fulfill professional audit responsibilities related to data security and forensics. Models in which the PHR-S is sponsored and housed by HIPAA entities are especially in need of this type of audit capability. However, audit capabilities are also needed for consumers. For example, a relevant consumer-facing audit report may list who has accessed PHR information, and when. **Examples:** - Security audit, which logs access attempts and resource usage including PHR Account Holder login, file access, other various activities, and whether any actual or attempted security violations occurred; - Data audit, which logs who, when, and by which system a PHR record was created, modified, viewed, extracted, or (if local policy permits) deleted; - Data exchange audit, which logs data exchanges between a PHR-S and other complementary electronic information systems (for example, sending application; the nature, history, and content of the information exchanged; outbound/received messages); and information about data transformations (for example, vocabulary translations and transmission and reception event details); - Audit-data may refer to: system setup data or clinical and patient management data; changes to the system clock.			8. The PHR-S **SHALL** audit data view according to user role, organizational policy, or jurisdictional law.	206
						9. The PHR-S **SHALL** audit object or data deletion according to user role, organizational policy, or jurisdictional law.	207
						10. The PHR-S **MAY** provide audit capabilities indicating the data value before a change.	208
						11. The PHR-S **SHALL** conform to function IN.3.3 (Entity Access Control) to limit access to audit record information to appropriate entities in accordance with user role, organizational policy, or jurisdictional law.	209
						12. The PHR-S **SHALL** provide the ability to generate an audit report in accordance with user role, organizational policy, or jurisdictional law.	210
						13. The PHR-S **SHOULD** provide the ability to view audit information related to a particular record or data set in accordance with user role, organizational policy, or jurisdictional law.	211
						14. The PHR-S **SHOULD** log PHR-S maintenance events for loading new versions of, or changes to, the PHR-S.	212
						15. The PHR-S **SHOULD** log PHR-S maintenance events for loading new versions of codes and knowledge bases.	213
						16. The PHR-S **SHOULD** log changes to the PHR-S system date and time where the PHR-S allows this to be done.	214
						17. The PHR-S **SHOULD** log system maintenance events for creating and restoring of backup.	215
						18. The PHR-S **SHOULD** log system maintenance events for archiving any data.	216
						19. The PHR-S **SHOULD** log system maintenance events for restoration of an archived PHR.	217

Copyright © 2008 HL7, All Rights Reserved

ID#	Type	Name	Statement/Description	See Also in EHR-S FM	See Also in PHR-S FM	Conformance Criteria	Row #
						20. The PHR-S **SHOULD** log beginning and ending of a system maintenance session.	218
						21. The PHR-S **SHOULD** log remote access connections including those for system support and maintenance activities.	219
						22. The PHR-S **SHOULD** utilize standardized time keeping (for example using the IHE consistent time profile for coordinating time across computer networks).	220
						23. The PHR-S **SHOULD** provide the ability to record and report upon audit information using a standards-based audit record format (for example RFC 3881).	221

Copyright © 2008 HL7, All Rights Reserved