



Personal Health Record Certification Criteria

09 First Draft Criteria

September 29, 2008

© 2008 The Certification Commission for Healthcare Information Technology

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments	Criteria Reference
								<p>P = Previous Criterion M = Modified N = New for Year R = Roadmap</p>	
PHR 01.01	PHR	Security: Access Control	The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Doctor etc.), or processes acting on behalf of users, for the performance of specified tasks.	09	N				SC 01.01 Markle CfH CT6
PHR 01.02	PHR	Security: Access Control	The system shall limit disclosures of identifying data to only those data that are necessary to perform the specified function(s) that the recipient is authorized to perform.	09	N				CFHC CT4 Criteria 1
PHR 02.01	PHR	Security: Audit Trail	The PHR-S shall provide audit capabilities indicating the data value before a change.				R		HL7 PHR Functional Model IN.4
PHR 02.02	PHR	Security: Audit Trail	PHR service or application shall maintain an audit trail with consumer's consents, with roll-back access to versions of applicable policies to the which the consumer consented.	09	N				Markle CfH CT3
PHR 02.03	PHR	Security: Audit Trail	PHR service or application shall provide the ability for consumers to access the audit trail report with the following minimum set of information: - Date and time the record was accessed - The person or party who accessed the record - Activities performed while accessing the record				R		
PHR 02.04	PHR	Security: Audit Trail	The system shall allow an authorized administrator to set the inclusion or exclusion of auditable events in SC 02.03 based on organizational policy & operating requirements/limits.				R		SC 02.01
PHR 02.05	PHR	Security: Audit Trail	The system shall explicitly label and manage the data in the PHR, and be able to discriminate between consumer and externally sourced data.	09	N				HL7 PH.2 Criteria 1 derivative HL7 PH 1 (p.7 and CMS Attach A 1.2.1)
PHR 03.01	PHR	Security: Authentication	When passwords are used, the system shall prevent the reuse of passwords previously used within a specific (configurable) timeframe (i.e., within the last X days, etc. - e.g. "last 180 days"), or shall prevent the reuse of a certain (configurable) number of the most recently used passwords (e.g. "last 5 passwords").	09	N				SC 03.12
PHR 03.02	PHR	Security: Authentication	The system shall support two-factor authentication in alignment with NIST 800-63 Level 3 Authentication. Note: The standards in this area are still evolving.				R		SC 03.13
PHR 03.03	PHR	Security: Authentication	The system, prior to access to any PHI, shall display a (configurable) warning or login banner (e.g. "The system should only be accessed by authorized users"). In the event that a system does not support pre-login capabilities, the system shall display the banner immediately following authorization.	09	N				SC 06.07

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments	Criteria Reference
								P = Previous Criterion M = Modified N = New for Year R = Roadmap	
PHR 04.01	PHR	Security: Data Storing	The system shall encrypt sensitive user data within the equipment that holds the data so as to prevent unauthorized access and disclosure in the case of a physical loss.	09	N				Markle CfH CT6
PHR 04.02	PHR	Security: Data Transmission	The system shall be able to communicate identity information across domains and web services using standards based user authentication and access control.			R			SC 07.01
PHR 05.01	PHR	Security: Identity Proofing	After successful identity proofing the user, the system shall provide the ability to issue a token or identifier to facilitate user authentication to the system.			R			Markle CFNPHR CT2
PHR 05.02	PHR	Security: Identity Proofing	The system shall provide the ability to perform identity proofing.			R			Markle CFNPHR CT2
PHR 05.03	PHR	Security: Identity Proofing	If identity proofing , token-issuing or on-going monitoring is outsourced, then there is a mechanism of audit and redress of third party as proof of chain of trust.			R			Markle CFNPHR CT2
PHR 05.04	PHR	Security: Identity Proofing	The system shall have strong mechanism in place for identifying the appropriate Health Data Source.			R			Markle CFNPHR CT2
PHR 05.05	PHR	Security: Identity Proofing	The system shall not use clinical data in the proofing process.			R			Markle CFNPHR CT2
PHR 05.06	PHR	Security: Identity Proofing	The system shall use at least Electronic Authentication Partnership (EAP) Level 2 Proofing Requirements including either in-person proofing or remote-proofing.			R			Markle CFNPHR CT2; EAF/EAP; NIST SP 800-63; NIST SP 800-53
PHR 06.01	PHR	Security: Interoperability	The system shall provide the ability to query systems requesting personal health information to insure the requesting system has the ability to protect masked data.			R			HL7 S.3.4 Criteria 3
PHR 06.02	PHR	Security: Interoperability	The system shall provide the ability to reject a request for transfer of data to other systems that do not support the ability to protect masked data.			R			HL7 S.3.4 Criteria 4
PHR 06.03	PHR	Security: Interoperability	The system shall provide the ability for the account holder to acknowledge receipt or denial of information sent from another system.			R			HL7 S.3.6 Criteria 8
PHR 06.04	PHR	Security: Interoperability	The system shall provide the ability to record confirmation of the target's receipt of the data.			R			HL7 S.4.1.2 Criteria 4
PHR 07.01	PHR	Security: Operations	Facilities that house equipment (e.g., servers, backup devices, etc.) that store health data must be physically secured and attended at all times. Access to such equipment should be limited to individuals who require it for authorized, legitimate, and documented (i.e., auditable) purposes.	09	N				Markle CfH CT6
PHR 07.02	PHR	Security: Operations	The system shall perform periodic or ongoing monitoring to prevent fraud and reduce risk of identity theft.	09	N				Markle CFNPHR CT2; NIST SP 800-100
PHR 07.03	PHR	Security: Technical Services	The software used to install and update the system, independent of the mode or method of conveyance, shall be certified free of malevolent software ("malware"). Vendor may self-certify compliance with this standard through procedures that make use of commercial malware scanning software.	09	N				SC 05.01

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 08.01	PHR	Security: Access Control	The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.	09	N				SC 01.02
PHR 08.02	PHR	Security: Access Control	The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role-based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)	09	N				SC 01.03
PHR 08.03	PHR	Security: Access Control	The system shall support removal of a user's privileges without deleting the user from the system. The purpose of the criteria is to provide the ability to remove a user's privileges, but maintain a history of the user in the system.	09	N				SC 01.04
PHR 08.04	PHR	Security: Access Control	If role-based access control (RBAC) is supported, the system shall be able to provide role based access control that is in compliance with the HL7 Permissions Catalog.				R		SC 01.05
PHR 08.05	PHR	Security: Access Control	If role-based access control (RBAC) is supported, the system must be capable of operating within an RBAC infrastructure conforming to ANSI INCITS 359-2004, American National Standard for Information Technology – Role Based Access Control.				R		SC 01.06
PHR 08.06	PHR	Security: Access Control	The system shall provide the ability to set the following proxy preferences: - Authorization to data (such as read-only, write-only, read/write, or read/write/edit) - Access to data types (e.g., access to all information, access only to medications, etc.) - Access to functions (e.g., send a message to a provider, grant/revoke proxy access to someone else, etc.)				R		???
PHR 08.07	PHR	Security: Access Control	The system shall enforce that individuals who access user data may only access the minimum amount of data necessary to fulfill their authorized purpose(s).				R		Markle CfH CT6
PHR 09.01	PHR	Security: Audit Trail	PHR service or application shall maintain an audit trail with the following auditable events: - Login attempts and their outcomes - Logout events, including timeouts - Granting and removal of access to others, including proxies and other systems and applications - Account status changes, including activation and deactivation of the account	09	N				Markle CfH CT3

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 09.02	PHR	Security: Audit Trail	The system shall be able to detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session timeout, account lockout, patient record created/viewed/updated/deleted, scheduling, query, order, node-authentication failure, signature created/validated, PHI export (e.g. print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.	09	N				SC 02.03
PHR 09.03	PHR	Security: Audit Trail	PHR service or application shall maintain an audit trail with the following auditable events: - Viewing of data - Creation of data - Modification of data - Deletion of data - Import of data from other systems or applications, including the source of such transaction - Export of data to other systems or applications, including the target of such transaction	09	N				Markle CfH CT3
PHR 09.04	PHR	Security: Audit Trail	Each entry in the audit trail of the PHR service or application shall identify the following: - The person or party who accessed the consumer's records, including the consumer, proxies, administrators, engineers, or any other parties or systems - Date and time for each access, including time-zone information - Actions performed - Data-source for each transaction involving transfer of data	09	N				Markle CfH CT3
PHR 09.05	PHR	Security: Audit Trail	The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.	09	N				SC 02.04

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 09.06	PHR	Security: Audit Trail	The system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. UTC synchronization).	09	N				SC 02.05
PHR 09.07	PHR	Security: Audit Trail	The system shall be able to support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.	09	N				SC 02.06
PHR 09.08	PHR	Security: Audit Trail	The system shall have the ability to format for export recorded time stamps using UTC based on ISO 8601. Example: "1994-11-05T08:15:30-05:00" corresponds to November 5, 1994, 8:15:30 am, US Eastern Standard Time.	09	N				SC 02.07
PHR 09.09	PHR	Security: Audit Trail	The system shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall prevent modifications to the audit records.	09	N				SC 02.08
PHR 09.10	PHR	Security: Audit Trail	The PHR-S shall provide the ability to view audit information related to a particular record or data set in accordance with jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.11	PHR	Security: Audit Trail	The PHR-S shall log remote access connections including those for system support and maintenance activities.	09	N				HL7 PHR Functional Model IN.4
PHR 09.12	PHR	Security: Audit Trail	The audit trail of the PHR application or service should be retained at minimum according to the data retention practice of the PHR application or service.	09	N				Markle CfH CT3
PHR 09.13	PHR	Security: Audit Trail	PHR service or application shall maintain an audit trail with consumer's revocation of consent.	09	N				Markle CfH CT3
PHR 09.14	PHR	Security: Audit Trail	The system shall provide the ability to report on the history of data submissions.	09	N				HL7 S.4.1.2 Criteria 5
PHR 09.15	PHR	Security: Audit Trail	The system shall provide the ability to record the date, data and target of the de-identified data.			R			HL7 S.4.1.2 Criteria 3
PHR 09.16	PHR	Security: Audit Trail	The system shall capture the source and date of a de-identified data request.			R			HL7 S.4.1.2 Criteria 2
PHR 09.17	PHR	Security: Audit Trail	The system shall provide the ability to record the requestor of the data including the date of request and the date of request determination.			R			HL7 S.3.7 Criteria 1
PHR 09.18	PHR	Security: Audit Trail	The PHR-S shall provide the ability to record and report upon audit information using a standards-based audit record format (for example RFC 3881).				R		HL7 PHR Functional Model IN.4
PHR 09.19	PHR	Security: Audit Trail	The PHR-S shall provide the ability to generate an audit report in accordance with user role, organizational policy, or jurisdictional law.	09	N				HL7 PHR Functional Model IN.4
PHR 09.20	PHR	Security: Audit Trail	The system shall provide a method for reporting disputes of data or transactions in the user's account.			R			Markle CFNPHR CT2

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 09.21	PHR	Security: Audit Trail	The system shall capture and store authorizations to receive data from or send data to an entity.			R			Markle CFNPHR CT2
PHR 09.22	PHR	Security: Audit Trail	The system shall provide immutable audit logs designating each specific proxy access and activities.			R			???
PHR 09.23	PHR	Security: Audit Trail	The PHR-S shall utilize standardized time keeping (for example using the IHE consistent time profile for coordinating time across computer networks).			R			HL7 PHR Functional Model IN.4
PHR 09.24	PHR	Security: Audit Trail	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.			R			HL7 PHR Functional Model IN.4
PHR 09.25	PHR	Security: Audit Trail	The PHR-S shall conform to function IN.3.1 (Entity Authentication).			R			HL7 PHR Functional Model IN.4
PHR 09.26	PHR	Security: Audit Trail	The PHR-S shall audit access to PHR-S according to user role, organizational policy, or jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.27	PHR	Security: Audit Trail	The PHR-S shall audit object or data creation according to user role, organizational policy, or jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.28	PHR	Security: Audit Trail	The PHR-S shall audit object or data modification according to user role, organizational policy, or jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.29	PHR	Security: Audit Trail	The PHR-S shall audit data extraction according to user role, organizational policy, or jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.30	PHR	Security: Audit Trail	The PHR-S shall audit data exchange according to user role, organizational policy, or jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.31	PHR	Security: Audit Trail	The PHR-S shall audit data view according to user role, organizational policy, or jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.32	PHR	Security: Audit Trail	The PHR-S shall audit object or data deletion according to user role, organizational policy, or jurisdictional law.			R			HL7 PHR Functional Model IN.4
PHR 09.33	PHR	Security: Audit Trail	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.			R			HL7 PHR Functional Model IN.4
PHR 09.34	PHR	Security: Audit Trail	PHR service or application shall maintain an electronic audit trail containing immutable entries that pertain to the consumer's account, information, and policy consent.			R			Markle CfH CT3
PHR 09.35	PHR	Security: Audit Trail	The system shall allow patient to view an immutable audit trail of all accesses and data transactions to their account.			R			Markle CFNPHR CT2
PHR 09.36	PHR	Security: Audit Trail	The system shall support logging to a common audit engine using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile.			R			SC 02.02
PHR 10.01	PHR	Security: Authentication	The system shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed, including when not connected to a network e.g. mobile devices.	09	N				SC 03.01
PHR 10.02	PHR	Security: Authentication	When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.	09	N				SC 03.02

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 10.03	PHR	Security: Authentication	The system upon detection of inactivity of an interactive session shall prevent further viewing and access to the system by that session by terminating the session, or by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.	09	N				SC 03.03
PHR 10.04	PHR	Security: Authentication	The system shall enforce a limit of (configurable) consecutive invalid access attempts by a user. The system shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).	09	N				SC 03.04
PHR 10.05	PHR	Security: Authentication	When passwords are used, the system shall provide an administrative function that resets passwords.	09	N				SC 03.05
PHR 10.06	PHR	Security: Authentication	When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.	09	N				SC 03.06
PHR 10.07	PHR	Security: Authentication	The system shall provide only limited feedback information to the user during the authentication.	09	N				SC 03.07
PHR 10.08	PHR	Security: Authentication	The system shall support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).	09	N				SC 03.08
PHR 10.09	PHR	Security: Authentication	When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rules.	09	N				SC 03.09
PHR 10.10	PHR	Security: Authentication	When passwords are used, the system shall support case-sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).	09	N				SC 03.10
PHR 10.11	PHR	Security: Authentication	When passwords are used, the system shall use Triple Data Encryption Standards (3DES), or Advanced Encryption Standards (AES) for encryption, and/or SHA1 or SHA 256 for hashing to store or transport passwords	09	N				SC 03.11
PHR 10.12	PHR	Security: Authentication	When passwords are used, the system shall not display passwords while being entered.	09	N				SC 06.02
PHR 10.13	PHR	Security: Authentication	The system shall authenticate all users and give access to only data they have been authorized to view.			R			Markle CFNPHR CT2
PHR 10.14	PHR	Security: Authentication	The system shall limit the number of consecutive and total attempts to enter a password.			R			Markle CFNPHR CT2
PHR 10.15	PHR	Security: Authentication	If system uses a password as a token, then the password shall be a "strong" password.			R			Markle CFNPHR CT2; NIST SP 800-63; NIST SP 800-12
PHR 10.16	PHR	Security: Authentication	The system shall provide separate logins or authentication for proxies.			R			???
PHR 11.01	PHR	Backup/Recovery	The system shall be able to generate a backup copy of the application data, security credentials, and log/audit files.	09	N				SC 08.01

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments	Criteria Reference
								P = Previous Criterion M = Modified N = New for Year R = Roadmap	
PHR 11.02	PHR	Security: Backup / Recovery	The system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.	09	N				SC 08.02
PHR 11.03	PHR	Security: Backup / Recovery	If the system claims to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.	09	N				SC 08.03
PHR 12.01	PHR	Security: Data Storing	The system, when storing PHI on any device intended to be portable/removable (e.g. thumb-drives, CD-ROM, PDA, Notebook), shall support use of a standards based encrypted format using triple-DES (3DES), or the Advanced Encryption Standard (AES), or their successors.	09	N				SC 06.06
PHR 12.02	PHR	Security: Data Storing	The system shall be configurable to prevent corruption or loss of data already accepted into the system in the event of a system failure (e.g. integrating with a UPS, etc.).	09	N				SC 05.02
PHR 13.01	PHR	Security: Data Transmission	The system shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPSec, XML encryptions, or S/MIME or their successors.	09	N				SC 06.01
PHR 13.02	PHR	Security: Data Transmission	For systems that provide access to PHI through a web browser interface (i.e. HTML over HTTP) shall include the capability to encrypt the data communicated over the network via SSL (HTML over HTTPS). Note: Web browser interfaces are often used beyond the perimeter of the protected enterprise network	09	N				SC 06.03
PHR 13.03	PHR	Security: Data Transmission	The system shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.	09	N				SC 06.04
PHR 13.04	PHR	Security: Data Transmission	The system shall support ensuring the authenticity of remote nodes (mutual node authentication) when communicating Protected Health Information (PHI) over the Internet or other known open networks using an open protocol (e.g. TLS, SSL, IPSec, XML sig, S/MIME).	09	N				SC 06.05
PHR 13.05	PHR	Security: Data Transmission	When the system uses HITSP TP13 (IHE XDS) as a Document Consumer, the system shall be able to use the TP13 "Document Integrity" option. This may be a configurable parameter or may be enabled at all times				R		SC 07.02
PHR 13.06	PHR	Security: Data Transmission	PHR service or application must be accountable for export and storage of information in applications that they have endorsed, whether those applications are browser-based or mobile devices.				R		Markle CfH CT6

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments	Criteria Reference
								P = Previous Criterion M = Modified N = New for Year R = Roadmap	
PHR 13.07	PHR	Security: Data Transmission	When information is presented to a user's web browser from equipment that holds this data (i.e., a data server), the system shall support the ability to ensure a secure transmission of the user's data, including use of encryption protocols such as Secure Socket Layer (SSL) technology.			R			Markle CfH CT6
PHR 13.08	PHR	Security: Data Transmission	The system shall comply with industry best practices for transmission of health data over the Internet even if they are not subject to information security regulations governing the health care industry.			R			Markle CfH CT6
PHR 14.01	PHR	Security: Documentation	The system shall include documentation that describes the patch (hot-fix) handling process the vendor will use for PHR, operating system and underlying tools (e.g. a specific web site for notification of new patches, an approved patch list, special instructions for installation, and post-installation test).	09	N				SC 04.01
PHR 14.02	PHR	Security: Documentation	The system shall include documentation that explains system error or performance messages to users and administrators, with the actions required.	09	N				SC 04.02
PHR 14.03	PHR	Security: Documentation	The system shall include documented procedures for product installation, start-up and/or connection.	09	N				SC 04.04
PHR 14.04	PHR	Security: Documentation	The system shall include documentation of the minimal privileges necessary for each service and protocol necessary to provide PHR functionality and/or serviceability.	09	N				SC 04.05
PHR 14.05	PHR	Security: Documentation	The system shall include documentation available to the customer stating whether or not there are known issues or conflicts with security services in at least the following service areas: antivirus, intrusion detection, malware eradication, host-based firewall and the resolution of that conflict (e.g. most systems should note that full virus scanning should be done outside of peak usage times and should exclude the databases.).	09	N				SC 04.06
PHR 14.06	PHR	Security: Documentation	The system shall include documentation that itemizes the services (e.g. PHP, web services) and network protocols/ports (e.g. HL-7, HTTP, FTP) that are necessary for proper operation and servicing of the system, including justification of the need for that service and protocol. This information may be used by the healthcare facility to properly configure their network defenses (firewalls and routers).	09	N				SC 04.08
PHR 14.07	PHR	Security: Documentation	The system shall include documentation that describes the steps needed to confirm that the system installation was properly completed and that the system is operational.	09	N				SC 04.09

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 14.08	PHR	Security: Documentation	The system shall include documentation available to the customer that provides guidelines for configuration and use of the PHR security controls necessary to support secure and reliable operation of the system, including but not limited to: creation, modification, and deactivation of user accounts, management of roles, reset of passwords, configuration of password constraints, and audit logs.	09	N				SC 04.10
PHR 14.09	PHR	Security: Documentation	The system shall include documentation of product capacities (e.g. number of users, number of transactions per second, number of records, network load, etc.) and the baseline representative configurations assumed for these capacities (e.g. number or type of processors, server/workstation configuration and network capacity, etc).			R			SC 04.03
PHR 14.10	PHR	Security: Documentation	If the system includes hardware, the system shall include documentation that covers the expected physical environment necessary for proper secure and reliable operation of the system including: electrical, HVAC, sterilization, and work area.			R			SC 04.07
PHR 15.01	PHR	Security: Functionality	The PHR should provide the ability to de-identify extracted information			R			???
PHR 15.02	PHR	Security: Functionality	The system shall provide the ability to identify specific PHR information to be reviewed and acted upon by the authorized account holder for the purpose of inactivation, destruction or retention.			R			HL7 S.3.7 Criteria 3
PHR 15.03	PHR	Security: Functionality	The system shall provide the ability to include account holder identifying information on each page of the reports generated.			R			HL7 S.3.7 Criteria 4
PHR 16.01	PHR	Security: Operations	Organizations hosting the PHR service or application personal health data shall require that require that all persons who have access to such data receive regular training and appropriate reminders about system security and the need to follow related protocols to protect the confidentiality of user information. In addition, policies should be in place (and regularly communicated) to handle persons who violate stated security protocols.			R			Markle CfH CT6
PHR 17.01	PHR	Security: System Maintenance	The PHR-S shall log PHR-S maintenance events for loading new versions of, or changes to, the PHR-S.				R		HL7 PHR Functional Model IN.4
PHR 17.02	PHR	Security: System Maintenance	The PHR-S shall log PHR-S maintenance events for loading new versions of codes and knowledge bases.				R		HL7 PHR Functional Model IN.4
PHR 17.03	PHR	Security: System Maintenance	The PHR-S shall log changes to the PHR-S system date and time where the PHR-S allows this to be done.				R		HL7 PHR Functional Model IN.4
PHR 17.04	PHR	Security: System Maintenance	The PHR-S shall log system maintenance events for creating and restoring of backup.				R		HL7 PHR Functional Model IN.4
PHR 17.05	PHR	Security: System Maintenance	The PHR-S shall log system maintenance events for archiving any data.				R		HL7 PHR Functional Model IN.4
PHR 17.06	PHR	Security: System Maintenance	The PHR-S shall log system maintenance events for restoration of an archived PHR.				R		HL7 PHR Functional Model IN.4

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments	Criteria Reference
								<div style="border: 1px solid black; padding: 2px;"> P = Previous Criterion M = Modified N = New for Year R = Roadmap </div>	
PHR 17.07	PHR	Security: System Maintenance	The PHR-S shall log beginning and ending of a system maintenance session.				R		HL7 PHR Functional Model IN.4
PHR 18.01	PHR	Interoperability	The system shall provide the ability to display CCD documents, using a subset of the HITSP C32 specification for Allergy and Conditions content information, and file them as intact documents in the PHR	09	N			Source-Conditions and Allergy Subset includes the following content modules of the HITSP C32: Person Information, Healthcare Provider, Condition, Allergies and Drug Sensitivity, Information Source, Comments	3.08 Summary Documents Using CCD Component (HITSP v2.1 2007 C32) Consumer Empowerment Interoperability Specification (HITSP v3.0 2007 IS03) Section 3.2.3.9 "Consumer-Document Display Subset" Consumer-Document Display (2008): requires the Document Consumer only to have the ability to display the document as requested. (it may not be able to locally import it in the patient record).
PHR 18.02	PHR	Interoperability	The system shall provide the ability to display CCD documents, using a subset of the HITSP C32 specification for Registration Summary information, and file them as intact documents in the PHR	09	N			Source-Registration Subset includes the following Content Modules of the HITSP C32 Document: Person Information, Language Spoken, Support, Healthcare Provider, Insurance Provider, Pregnancy, Information Source, Comments, Advance Directives	3.08 Summary Documents Using CCD Component (HITSP v2.1 2007 C32) Consumer Empowerment Interoperability Specification (HITSP v3.0 2007 IS03) Section 3.2.3.9 Consumer-Document Display Subset Consumer-Document Display (2008): requires the Document Consumer only to have the ability to display the document as requested. (it may not be able to locally import it in the patient record).
PHR 18.03	PHR	Interoperability	The system shall provide the ability to display CCD documents, using a subset of the HITSP C32 specification for Medication and Immunization History information and file them as intact documents in the PHR	09	N			Source-Medication Subset includes the following content modules of the HITSP C32: Person Information, Healthcare Provider, Medications-Prescriptions and Non-Prescription, Information Source, Comments	Summary Documents Using CCD Component (HITSP v2.1 2007 C32) Consumer Empowerment Interoperability Specification (HITSP v3.0 2007 IS03) Section 3.2.3.9 "Consumer-Document Display Subset" Consumer-Document Display (2008): requires the Document Consumer only to have the ability to display the document as requested. (it may not be able to locally import it in the patient record).
PHR 18.04	PHR	Interoperability	The system shall provide the ability to accommodate the exchange of its data contents to another PHR system.			R			AHIC Use Cases -Consumer Empowerment and Emergency Responder (HITSP C32 v. 2.1, table IS-03 and IS-04)

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 18.05	PHR	Interoperability	The system shall provide the ability to accommodate the exchange of account holder-defined data with an EHR-S.			R			HL7 S.3.6 Criteria 1
PHR 18.06	PHR	Interoperability	The system shall provide the ability to accommodate the exchange of account holder-defined data with other systems.			R			HL7 S.3.6 Criteria 2
PHR 18.07	PHR	Interoperability	The system shall provide the ability for the PHR account holder to designate entities from which data will be exported from the PHR.			R			HL7 S.3.6 Criteria 3
PHR 18.08	PHR	Interoperability	The system shall provide the ability for the PHR account holder to exchange information with an entity on a one-time basis.			R			HL7 S.3.6 Criteria 5
PHR 18.09	PHR	Interoperability	The system shall provide the ability to export and/or make viewable PHR records using various platforms without needing special viewing software (e.g., browser).			R			HL7 S.3.6 Criteria 6
PHR 18.10	PHR	Interoperability	The PHR shall provide the ability to use standard terminologies and terminology models associated with the minimum data set to communicate with other PHRs.			R			HL7 S.3.7 Criteria 5
PHR 18.11	PHR	Interoperability	The system shall support interoperable data exchange protocols among ECONs for the minimum data set.			R			
PHR 18.12	PHR	Interoperability	The system shall support recurring, standing requests for PHR information.			R			
PHR 18.13	PHR	Interoperability	The system shall support 'masking' as part of any PHR provided.			R			HL7 S.3.7 Criteria 4
PHR 18.14	PHR	Interoperability	The PHR shall provide the ability to extract (or selectively import) health record information				R		HL7 S.3.7 Criteria 8
PHR 18.15	PHR	Interoperability	The system shall provide the ability to use interoperability standards as required by realm specific and/or local profiles.				R		
PHR 18.16	PHR	Interoperability	The system should have the ability to synchronize a minimum data set with another system.				R		HL7 PHR FM: IN2 Standards Based Interoperability
PHR 18.17	PHR	Interoperability	The system shall request delivery confirmation from a system external to the PHR system whenever information is sent by the PHR system to that system.			R			
PHR 18.18	PHR	Interoperability	The system shall log and maintain a record of each delivery confirmation request that it sends to a system external to the PHR system, and each delivery confirmation it receives in response.				R		
PHR 18.19	PHR	Interoperability	The system shall provide confirmation to a system external to the PHR system whenever that system requests confirmation that information it sent was accepted by the PHR system.				R		
PHR 18.20	PHR	Interoperability	The system shall log and maintain a record of each delivery confirmation request it receives from a system external to the PHR system, and each delivery confirmation it sends in response.				R		
PHR 18.21	PHR	Interoperability	The system shall provide the ability to use different versions of interoperability standards.				R		

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 18.22	PHR	Interoperability	The system shall provide the ability to change (reconfigure) the way data is transmitted as an interoperability standard evolves over time and in accordance with business needs.				R		
PHR 18.23	PHR	Interoperability	The system shall provide the ability to retire and replace an interoperability standard.				R		
PHR 18.24	PHR	Interoperability	The system shall provide the ability to be interoperable with other ECONs, PHRs, or EHRs that use known earlier versions of an interoperability standard.				R		
PHR 18.25	PHR	Interoperability	The system shall provide mechanisms for the consumer to export information from his/her account in standard formats.			R			
PHR 18.26	PHR	Interoperability	The system shall have a menu of output formats that are both human-usable and machine-readable.			R			Markle
PHR 18.27	PHR	Interoperability	The system shall provide a warning message to the account holder with a means to download information before information is no longer accessible. (the first one might cover this.)				R		
PHR 18.28	PHR	Interoperability	The system shall provide the ability for the PHR account holder to designate entities from which data will be imported into the PHR.				R		
PHR 19.01	PHR	Privacy: Account Management	If the PHR contains data from new external sources for which consent has not already been given, the system shall provide the ability for an account holder to terminate her account and prevent source information from auto-populating the PHR.	09	N			LINKED model, opt-out scenario	
PHR 19.02	PHR	Privacy: Account Management	The PHR shall provide the ability for the consumer to explicitly opt-in / opt-out of PHR use	09	N			LINKED model	
PHR 19.03	PHR	Privacy: Account Management	PHR service or application shall provide the ability for the consumer to open, close, or transfer their account			R			HL7 PHR FM PH 1.6 variation
PHR 19.04	PHR	Privacy: Account Management	PHR service or application shall provide the ability to confirm to the consumer when they open, close, or transfer their account			R			HL7 PHR FM PH 1.6 variation
PHR 19.05	PHR	Privacy: Account Management	The system shall allow the user to expunge their record.			R			
PHR 20.01	PHR	Privacy: Conditions of Use	The system shall require the account holder to agree to the Conditions of Use when the system is initially used by the account holder.	09	N			BOTH	HL7 S.3.2 Criteria 1
PHR 20.02	PHR	Privacy: Conditions of Use	The system shall provide an initial notification to the account holder regarding the Conditions of Use and subsequent notifications if changes are made.	09	N			BOTH	HL7 S.3.2 Criteria 2
PHR 20.03	PHR	Privacy: Conditions of Use	The system shall provide the ability to view and print the Conditions of Use.	09	N			BOTH	HL7 S.3.2 Criteria 4
PHR 20.04	PHR	Privacy: Conditions of Use	The system shall provide the ability for the account holder to report to the Personal Health Records sponsor(s) as part of the process to seek redress for the sponsor's failure to meet performance expectations as specified in the Conditions of Use agreements.	09	N			BOTH	HL7 S.3.2 Criteria 5

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments P = Previous Criterion M = Modified N = New for Year R = Roadmap	Criteria Reference
PHR 21.01	PHR	Privacy: Consent	If the PHR contains data from external sources for which consent has not already been given, the PHR shall obtain the consumer's consent prior to collecting, displaying, accessing, storing, releasing, disclosing or using identifiable personal health information when received <u>directly from the consumer</u> except where jurisdictional law presides.	09	N			LINKED THIS IS NOT INTERNALLY CONSISTENT	CfH Markle Common Framework for Networked Personal Health Information, CP2 & CP3
PHR 21.02	PHR	Privacy: Consent	PHR service or application shall provide notice to consumers about privacy practices and policies for collecting, displaying, accessing, storing, releasing, disclosing or using identifiable personal health information	09	N			BOTH	CfH Markle Common Framework for Networked Personal Health Information, CP2 & CP3
PHR 21.03	PHR	Privacy: Consent	PHR service or application shall provide the ability to capture, display and print that a consumer has granted, withheld or revoked their privacy consent	09	N			BOTH (similar to 23.05 - duplicate?)	HL7 PHR FM PH 1.3 variation
PHR 21.04	PHR	Privacy: Consent	PHR service or application shall provide the ability to capture, display and print documentation related to assent for the account holder legally unable to offer privacy consent dependent on organizational policy and jurisdictional law				R		HL7 PHR FM PH 1.3 variation
PHR 21.05	PHR	Privacy: Consent	The system shall provide the ability to define an entity to which the Consent or Authorization applies.	09	N			BOTH	HL7 S.3.3.1 Criteria 3
PHR 21.06	PHR	Privacy: Consent	The system shall provide the ability for the account holder to select the entity or clinician to which the Consent or Authorization applies.	09	N			BOTH	HL7 S.3.3.1 Criterion 2 - derivative
PHR 21.07	PHR	Privacy: Consent	The system shall provide the ability to identify a section or sections that are consistent with jurisdictional law and to which the Consent or Authorization applies.	09	N			LINKED	HL7 S.3.3.1 Criteria 4
PHR 21.08	PHR	Privacy: Consent	The system shall provide the ability for the account holder to set specific access rights to specific sections of the PHR for each actor in the registry	09	N				HL7 PH.3.5.3 Criterion 2
PHR 21.09	PHR	Privacy: Consent	The system shall provide the ability to identify individual elements of records to which the Consent or Authorization applies.				R		HL7 S.3.3.1 Criteria 5
PHR 21.10	PHR	Privacy: Consent	The system shall provide the ability to define the time period within which the Consent or Authorization applies.				R		HL7 S.3.3.1 Criteria 6
PHR 22.01	PHR	Privacy: Consent	PHR service or application shall provide the ability to capture, display and print the privacy consent including the account holder or their personal representative if the account holder is legally unable to offer or provide it				R		HL7 PHR FM PH 1.3 variation
PHR 22.02	PHR	Privacy: Consent Management	PHR service or application shall manage and update consumer privacy consents maintaining version control on-line	09	N			BOTH	HL7 PHR FM PH 1.5 variation
PHR 22.03	PHR	Privacy: Consent Management	PHR service or application shall provide the ability to chronologically display consumer privacy consents on-line				R		HL7 PHR FM PH 1.5 variation
PHR 22.04	PHR	Privacy: Consent Management	The system shall provide the ability to capture Consents and Authorization through electronic interfaces such as scanning or faxing.				R		HL7 S.3.3.1 Criteria 8
PHR 22.05	PHR	Privacy: Consent Management	PHR service or application shall provide the ability to store, display and print consumer privacy consents from on-line	09	N			BOTH (similar to 22.03 - duplicate?)	HL7 PHR FM PH 1.5 variation

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments	Criteria Reference
								<div style="border: 1px solid black; padding: 2px;"> P = Previous Criterion M = Modified N = New for Year R = Roadmap </div>	
PHR 23.01	PHR	Privacy: Consent Management - Proxy	The system shall enable proxies to be easily revocable.			R			
PHR 24.01	PHR	Privacy: Patient - Provider Communications	The system shall provide the ability to capture, index and store documentation of communications between providers and the account holder and/or the account holder's representatives.			R			HL7 PH.6.3 Criterion 1
PHR 25.01	PHR	Privacy: Patient - Provider Communications Access Control	The system shall provide the ability to capture, index and store documentation regarding family member or account holder representative or clinicians authorizations to receive account holder related health information.	09	N			duplicate with Security 08.01	HL7 PH.6.3 Criterion 4
PHR 26.01	PHR	Privacy: Access Control	The PHR shall permit the account holder to define PHR information as private, and restrict views of such data.	09	N				
PHR 26.02	PHR	Privacy: Access Control	If it contains data from external sources that consent has not already been gathered, then PHR service or application shall obtain the consumer's consent prior to collecting, displaying, accessing, storing, releasing, disclosing or using identifiable personal health information when received <u>on behalf of consumer</u> e.g. health care providers, employers or health plans or third party entities except where jurisdictional law presides.	09	N				CiH Markle Common Framework for Networked Personal Health Information, CP2 & CP3
PHR 26.03	PHR	Privacy: Access Control	PHR service or application shall provide the ability to capture, display, maintain and make available the consumer's privacy consent decisions and preferences such as who sees what PHI and under what circumstances			R			HL7 PHR FM PH 1.5 variation
PHR 27.01	PHR	Privacy: Proxy Management	PHR service or application shall provide the ability to document the account holder's personal representative's authority to make decisions on behalf of the account holder			R			HL7 PHR FM PH 1.3 variation
PHR 28.01	PHR	Privacy: Record Amendment	The system shall provide account holders the ability to request an amendment by email and provide a phone number on the site to reach customer service.	09	N			BOTH	
PHR 29.01	PHR	Privacy: Third-party access and use	PHR service or application shall provide the ability for the consumer to opt-in for sharing their PHI as deidentified data			R			CiH Markle Common Framework for Networked Personal Health Information, CP2 & CP3
PHR 29.02	PHR	Privacy: Third-party access and use	PHR service or application shall provide the consumer with the ability to specify what information can be shared with external sources such as researchers			R			CiH Markle Common Framework for Networked Personal Health Information, CP2 & CP3
PHR 29.03	PHR	Privacy: Third-party access and use	The system shall maintain a registry of all actors and organizations have access to the PHR including data providers that import information into the PHR.	09	N				HL7 PH.3.5.3 Criterion 1

Criteria #	Certification Track	Category	Criteria	Year introduced or last modified	09 Certification	10 Roadmap	11+ Roadmap	Comments	Criteria Reference
								<div style="border: 1px solid black; padding: 2px;"> P = Previous Criterion M = Modified N = New for Year R = Roadmap </div>	
PHR 29.04	PHR	Privacy: Third-party access and use	<p>The PHR service or application shall develop and maintain proof of binding contractual Chain of Custody Agreements with its third party entities.</p> <p>The Chain of Custody Agreement must include the following:</p> <ul style="list-style-type: none"> - Terms by which it shares or exchanges personally identifiable, partially identifiable, or de-identified data with third party entities - Prohibitions against re-identification of de-identified data without consent of the consumer. - Explicit documentation of agreements with third party entities that involves transfer or sale of consumer information. - The process by which the consumer will be contacted in the event of a violation of the Chain of Custody Agreement. <p>This shall be readily accessible by the consumer.</p>			R			
PHR 29.05	PHR	Privacy: Third-party access and use	The system shall allow the account holder to de-identify his or her information as needed to meet the requirements of a study or other request.			R			HL7 S.4.1.2 Criteria 1
PHR 29.06	PHR	Privacy: Third-party access and use	The system shall capture the source and date of a de-identified data request.			R			HL7 S.4.1.2 Criteria 2
PHR 29.07	PHR	Privacy: Third-party access and use	The system shall provide the ability to record the date, data and target of the de-identified data.			R			HL7 S.4.1.2 Criteria 3
PHR 29.08	PHR	Privacy: Third-party access and use	The PHR should provide the ability to extract data for administrative purposes as authorized by the account holder			R			
PHR 29.09	PHR	Privacy: Third-party access and use	The PHR should provide the ability to extract data for research purposes as authorized by the account holder			R			
PHR 29.10	PHR	Privacy: Third-party access and use	The PHR should provide the ability to extract data quality analysis purposes as authorized by the account holder			R			
PHR 29.11	PHR	Privacy: Third-party access and use	The PHR should provide the ability to extract data for public health purposes as authorized by the account holder			R			
PHR 30.01	PHR	General Functionality: Manage Account Holder Provider's Information	The system shall provide the ability to capture account holder provider contact information.	09	N				HL7 S.1.2 - criterion 1
PHR 31.01	PHR	General Functionality:	The system shall provide the ability for the account holder to record his or her own health observations (i.e., symptoms, vital signs, physical observations, home laboratory studies such as blood sugars).	09	N				HL7 PH.3.1.1 criterion 1