Personal Health Records: Technical Considerations
PHRs: Technical Considerations

• The purpose of this presentation is to provide the HIMSS membership with an overview of those technical requirements that should be considered when evaluating Personal Health Records (PHR) solutions.

• The contents of this presentation are the result of the efforts of the PHR Technical Work Group that reports to the HIMSS PHR Steering Committee. The efforts were conducted from January through April, 2009.
  – The Workgroup team was: Lucy Mancini Newell; Lory Wood, Penny Back, Kate Christensen, Michael Wilson, Brian Wells, Charles Tuchinda, Mary Griskewicz and David Fitzgerald
PHRs: Technical Considerations

• The discussion on PHR technical considerations begins with a conceptual model that graphically represents those technical elements that should be considered by any healthcare organization that is contemplating this type of initiative. Those technical requirements identified in the conceptual model on the following page include:
  – Standards
  – Interoperability
  – Security and Privacy
  – Application Architecture
  – Data Integration
  – System Architecture
  – Reporting
  – Technical Support

• **Note:** Please note that terminology may vary by organization. We have made every attempt to develop a starter set of information that can be augmented as needed.

• **Source of many requirements are from the:** HL7 Personal Health Record System (PHR-S) Functional Model [http://www.hl7.org/ehr/](http://www.hl7.org/ehr/).
PHR Information Technology Considerations

Security & Privacy  Interoperability  Standards

Application Architecture

Data  System Architecture  Reporting  Technical Support

Patient / Consumer

(Conceptual Model)
Ask Yourself: Does the PHR System?

Support a formal standard terminology model.

Support standard formats for data exchange.

Support the ADA (Americans with Disabilities Act)? Adhere to 508 compliance.

Employ standard terminologies to ensure data correctness and to enable semantic interoperability (both within an enterprise and externally).

Understand product uses any of standards and conventions.
PHRs: Additional Standards Considerations

- Understand the solution's tools, methods, and user interfaces are intuitive and conducive to rapid configuration and implementation, as well as "easy to use" for the end user.
- Consistent user interfaces and user paradigms are some ways to achieve standardization.
  1. Understand the solution’s approach and implementation in this area.
  2. Does the solution follow any human factors engineering guidelines?
Ask Yourself: Does the PHR System Understand?

- The typical response time for the PHR application start-up for users.
- Log in times.
- Application screen-to-screen navigation.
- The factors that would affect the PHR system response times.

Interoperability
PHRs: Additional Interoperability Considerations

- Understand the benchmarks for your largest healthcare installation or largest customer. Benchmarks should indicate number of concurrent users, database size (and RDBMS product), number of transactions per period, etc.
- Understand the performance and response time measured for your product?
- Describe your load balancing strategy at both the web and application tiers.
- Understand the maximum number of concurrent I/Os to the database, for each RDBMS product used.
- Understand the factors within your product affect response time?
- Understand the built-in functionality is available for assessing performance of specific transactions/workflow?
- Understand how the system achieves scalability.
Ask Yourself: Does the PHR System?

- Manage the sets of access control permissions granted.
- Secure the access to a PHR SYSTEM and PHR information.
- Prevent unauthorized use of data, data loss, tampering and destruction.
- View confidential data or authentication data (e.g., password, pin, SSN) is it captured in any of the audit trails.
- Provide the ability to restrict access to, as well as the use and disclosure of, data according to user roles, organizational policy, or jurisdictional law.
PHRs: Additional Security Considerations

- Encrypt data during network transport and data transmission between application tiers.
- Provide the ability for the Individual to restrict access to demographic information or any other data or fields in the PHR.
- Provide Individual data in a manner that meets local requirements for de-identification.
- Manage the health record information according to user role, and as applicable, organizational policy, or jurisdictional law.
- Enable Individuals to extend partial or full access to PHR information to other individuals who can act on behalf of the Individual (proxy users), clinicians, systems, and others.
- Enable Individuals to deny access to PHR information.
- Enable Individuals to determine what information, may be accepted into an Individual's PHR.
- Understand how support personnel access the systems when providing remote support?
- Understand what integrity checks are employed to prevent corruption of the database(s) and local files?
- Understand the options available for logging user and workflow activity.
- Understand if your system has the ability to support remote access.
- Understand details of operating system, firewall, network, and application level transaction logging and integration opportunities for disparate log sources.
- Understand data encryption for data at rest? If yes, what software/standards are used and supported? Where in the solution is it used and at what level of encryption?
- Maintain consents and authorization directives/statements for any entity that may or may not have access to the Individual's PHR.
- Verify and enforce access control to all PHR SYSTEM components, PHR information and functions for end-users, applications, sites, etc., to prevent unauthorized use of a resource.
Ask Yourself: Does the PHR System?

Identify physical components of the system (i.e., hardware and operating systems used on each server or processing node).

Use terms like: “configuration” vs. “customization” to achieve functional flexibility, understand how it might cost you either in labor or programming dollars.

Identify the technology options for the user interface (e.g., a browser interface or software that resides on the desktop). If more than one technology is used, know what your user community interface technology needs.

Contain any freeware or shareware? Understand where and how the freeware/shareware is used.

Contain any Open Source software (e.g., JBOSS, Apache)? If so, understand how Open Source products may impact your existing system and license agreements.
PHRs: Additional Application Architecture Considerations

• Does the product integrate with web portal technology? If so, with which specific product(s) is it integrated (e.g., IBM WebSphere Portal Server)?
• Understand if the product installs software on the end-user's PC: does the product require or assume that any DLLs, OCXs, JREs or other software components reside on the PC, other than the core product?
• Understand if the product installs software on the user's PC: does the product install any DLLs, OCXs, JREs on the user's PC as part of the core system, or require that these be installed in order to run the system?
• Understand the scope of configurations that control functions and access within your applications that will be maintained.
• Understand the extent of customization typically required by a client.
• Understand the product support load balancing? If so, please describe how.
• Understand if the product handles session management?
• Understand if the product supports both real-time and batch interfaces. Please describe its capabilities with regards to these two types of integrations.
• Understand any integration capabilities with middleware products (e.g., TIBCO, WebSphere). Are there solution adapters with middleware vendor products that can be used for integration?
Ask Yourself: Does the PHR System?

- Provide the ability to indicate that a patient has granted, withheld or revoked access to applicable consent directives and authorizations.
- Provide the ability to uniquely identify an Individual and tie the record to an Individual.

Manage Patient Originated Data.

- Provide the ability to document the individual’s personal representative’s authority to make decisions on behalf of the Individual.

- Provide audit capabilities for system access and usage indicating who accessed the record, when, what actions were taken, and when the actions occurred.
PHRs: Additional Systems Architecture Considerations

- The system Should associate key identifier information (e.g., medical record number, insurance account number, and voluntary unique identifiers) with each Individual.
- The system Should provide the ability to capture, present, maintain and make available for healthcare decisions patient preferences such as language, religion, spiritual practices or culture.
- The system Should provide the ability to indicate the type of advance directives completed for the Individual such as living will, durable power of attorney, preferred interventions for known conditions, organ donation, or the existence of a "Do Not Resuscitate order” or organ donation preferences in accordance with organizational policy, scope of practice, or jurisdictional law.
- The system Should provide the ability to manage Individual and/or family preferences as they pertain to current treatment plans.
- The system should be available e.g. 95% of the time, 7 days a week, 24 hours a day.
- Enable standards-based application integration.
- Enable version control according to customized policies to ensure maintenance of utilized standards.
- This includes the ability to accommodate changes to terminology sets as the source terminology undergoes its natural update process (new codes, retired codes, redirected codes). Such changes need to be cascaded to clinical content embedded in templates, custom formularies, etc., as determined by local policy.
- The system should Produce and Present  Ad Hoc Views of the Personal Health Record
Ask Yourself: Does the PHR System Understand?

- All the data interchanges with third party vendors that may be part of the PHR System. For each interchange, know whether each interchange is batch or real-time.

- Data extraction capabilities, (e.g., data aggregation, in accordance with data exchange, analysis, reporting and printing requirements).

- How interactions between third party systems authenticated.

- Multi-channel support for users and understand the technical requirements for email, fax, imaging, correspondence generation, desktop/local print, system print, other output management systems.

- Electronic attestation of attestable information including the retention of the signature of attestation (or certificate of authenticity) associated with incoming or outgoing information.

- How appropriate identity checks are being conducted before data is linked or transferred between PHR/EHR systems.
PHRs: Additional Data Considerations

- Explain PHR data is: Captured, stored, secured, messaged, displayed and reported.
- Ensure information entered by or on behalf of an Individual is accurate and logged.
- The system should store historical values of demographic data over time.
- The system should manage historical and current state data.
- Manage information related to self-assessments.
- Incorporate genomic/proteomic data and documentation from external sources.
- Understand the process for archiving and purging data.
- Can multiple users access and/or update records at the same time? If so, how do you prevent record locking?
- Communication with Medical Devices
- To capture provider assessments and their supporting documentation such that the Individual or another provider may independently review the assessments.
Ask Yourself: Does the PHR System?

Work with other 3rd party reporting tools that may be purchased separately?

Understand the views of the PHR information, in accordance with user roles, organizational policies and jurisdictional laws as related to privacy and confidentiality.

Understand the reporting and query capabilities of your product, including the scope of the data that can be included, and the technologies used to generate the reports and queries.

Support the delivery of reports via http?

Have a data dictionary or other facility to assist end users or IT users in defining reports?

Understand reporting functions part of the base application or a separate application?
Ask Yourself: Define the PHR System Service Level Agreement?

- Define the scope of functions that are maintained only by you.
- Define the company’s process and timeliness for gathering, prioritizing, and developing client-recommended enhancements.
- Define how third parties conform to HIPAA security and privacy regulations.
- Define if and how the PHR solution could be “hosted” by you?
- Define plans for future technology enhancements.
- Define the type and level of ongoing support to be provided on a continuing basis for system software and application software problems and questions.
PHRs: Additional Technical Support Considerations

- Understand the process of recording, prioritizing, and fixing software bugs.
- Understand the usual pace of releases, usual number of back versions supported, and usual time requirements for upgrading.
- Understand how product support web-based (or other) training for users?
- Understand what documentation is provided for administration of your application, including security, engineering and development, as applicable.
- Understand any facilities necessary in order to troubleshoot and correct software problems.
- Understand the recent history of system enhancements.
- Understand how frequently virus signatures updated? What software is used for virus detection?
- Understand if there is the ability for the solution to support 24x7 operations? If so, please detail how the technology solution would be able to support this from an implementation and configuration perspective.
- Understand if users are blocked after a configurable number of incorrect password attempts?
- Understand what rules govern password selection (e.g., minimum/maximum length, content restrictions, historical retention per user) and reset? Are passwords forced to expire at set intervals? Do users select their own passwords? How do users change their passwords?