1. Privacy and Security and Emerging Technologies

What privacy and security risks, concerns, and benefits arise from the current state and emerging business models of PHRs and related emerging technologies built around the collection and use of consumer health information, including mobile technologies and social networking?

A wide range of PHR technologies is available today as is a correspondingly wide and valid set of PHR definitions. While this broadness in both PHR technology and definition is inclusive and accommodating, it may exponentially increase the number of possible privacy and security-related scenarios and concerns that must be addressed by any approaches adopted by ONC.

A number of highly relevant, consensus-based HIT standards are available not only to help mitigate these concerns and risks but to promote the immediate usefulness of PHR data. HL7's PHR-System Functional Model (PHR-S FM), for example, provides definitions for capabilities of PHR systems and offers a standards-based way of identifying and addressing many of the concerns raised by healthcare professionals and consumers, including:

- Import and reuse of professionally-sourced data
- Capture of consumer-sourced data
- Use and reuse of Protected Health Information
- Care collaboration between healthcare professionals
- Security and Confidentiality
- Consents and authorizations
- Consumer's ability to manage and control access to the data
- Auditability / traceability
- Etc.

Developed with input from HL7's 30+ international affiliates, HL7's PHR-S FM is both policy agnostic and representative of emerging models around the world. HL7 plans to seek both ANSI and ISO normative approval for the standard in 2011, thereby providing consumers, providers, payers, and vendors with a single set of terms that are relevant and consistent across borders and countries.

HL7's Security and Community Based Collaborative Care Work Groups have developed standards and artifacts that compliment and support the PHR-S FM in a technology-neutral manner. For example, HL7's Composite Privacy Consent Directive Draft Standard provides a model for describing common elements across policies in a standard-based and interoperable form that is implementation-neutral. Since the standard may be used to author both privacy policies and privacy consent directives, the criteria used to specify sensitive information is consistent across policies and privacy consent.

The initial version of this standard, which was based on HL7's Version 2.x messaging standard, has been successfully adopted in British Columbia, Canada. The current version of the standard is based on HL7's Clinical Document Architecture (CDA), a document-

based standard. A Consent Directive Clinical Document Architecture (CDA) Implementation Guide is now available to assist implementers.

Additional information about these standards and other work within HL7 to support electronic privacy policies and consent directives, is provided as Appendix A to this document. HL7 encourages both current state and emerging business model and technologies to take advantage of these standards

2. Consumer Expectations about Collection and Use of Health Information

Are there commonly understood or recognized consumer expectations and attitudes about the collection and use of their health information when they participate in PHRs and related technologies? Is there empirical data that allows us reliably to measure any such consumer expectations? What, if any, legal protections do consumers expect apply to their personal health information when they conduct online searches, respond to surveys or quizzes, seek medical advice online, participate in chat groups or health networks, or otherwise? How determinative should consumer expectations be in developing policies about privacy and security?

HL7 recognizes that there is a wide range of consumer expectations. Younger generations, for example, seem more comfortable with sharing data. The Markle Foundation and the American Medical Association have both hosted surveys to measure consumer expectation. Other surveys such as the one posted by the California Health Care Foundation (http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey) may also provide useful insights.

Regarding legal protections expected by consumers when supplying personal health information to conduct online searches, respond to surveys or quizzes, seek medical advice online, participate in chat groups or health networks, or other activities, these functions may be invoked within a PHR System or not. For example, if a consumer uses a major vendor's private portal, all of the above are expected to be maintained and accessible only by the PHR account holder.

It may be difficult to determine consumer expectations if PHR capabilities and definitions of PHI are not widely understood in the community. As indicated above, HL7's PHR-S FM can easily be accessed by the public to facilitate thinking on the scope of capabilities that could be applied to privacy and security policies. The HL7 PHR-S FM already has broad uptake and, as it proceeds through both ANSI and ISO approval, will truly be representative of a global audience. A summary of HL7's PHR-S FM is provided as Appendix B to this document

3. Privacy and Security Requirements for Non-Covered Entities

What are the pros and cons of applying different privacy and security requirements to non-covered entities, including PHRs, mobile technologies, and social networking?

PROs
Flexibility for consumers to choose how they wish to manage and control their PHR health information, and they may have more choices among non-covered PHRs than ones controlled by a HIPAA Covered Entity.

CONs
One of the disadvantages to applying privacy and security requirements to non-covered entities that differ from HIPAA requirements is that most consumers assume that different technologies have or should have a similar set of capabilities; they simply consider these technologies as different but similar means to access the same information. As noted in the response to the first question, variation, while inclusive, may complicate privacy and security policies about which consumers will need to be knowledgeable, and may raise trust and data integrity issues for both providers and consumers. The differing privacy and security requirements may add costs to vendors supplying technologies to both the covered and non-covered entity markets

Generally, it is not clear whether differing privacy and security requirements will inhibit or promote PHR adoption. In and of itself, uniformity at the federal level will not change the fact that there are numerous other privacy and security laws and policies, which will continue to differ unless there is a massive preemption of these laws and a dramatic narrowing of the policy discretion currently afforded covered entities under HIPAA privacy and security rules.

The key to ensuring that consumers adopt PHRs is to make their ability to manage and control the use of their health information as transparent and user-friendly as possible. The key to gaining provider confidence in the information that their patients share with them is to automate the enforcement of privacy and security requirements so that care delivery is not hampered by the differences.

Adoption of HL7 standards that enable exchange of encoded privacy and security policies and the computable adjudication of these policies and patient consent directives as personal health information moves from one data user to the next will allow the differing requirements and policies to be transparent and provide a means for aligning them. HL7 stands ready to provide standards for enabling and managing trust and maintaining data integrity regardless of the scenario, and would like to work with ONC to fulfill these needs.

4. Any Other Comments on PHRs and Non-Covered Entities
Do you have other comments or concerns regarding PHRs and other non-covered entities?

HL7 is aware of concerns regarding the assumption of non-alterability of professionally sourced data and also concerns about patients facing a plethora of different PHRs, one for each provider, health plan, etc.

While it is outside the scope of a Standards Developing Organization such as HL7 to advocate for certification of PHR systems, should ONC and NIST decide to create a certification program, HL7 can support this program with several of its existing standards including the PHR FM. Should ONC decide that the PHR Framework includes a certification component, HL7 can offer a standards-based platform that recognizes and supports the benefits of certification, and mitigates the associated risks.

Other activities ONC might consider undertaking:

- Creating a PHR Framework that provides structured documentation or model of the various types of PHR data capture and exchange, the types of standards, governance, and participant roles involved
- Creating incentives that promote adoption of standards-based certified PHR systems to increase the level of confidence in PHR systems.

HL7 appreciates the opportunity to comment on and provide input to the discussions around PHRs and their corresponding privacy and security issues, and looks forward to working with ONC to create solutions to benefit the industry as a whole.

Appendix A:
HL7 Standards Supporting Electronic Privacy Policies and Consent Directives

HL7 Community Based Collaborative Care Work Group (CBCC WG) had developed several standards in support of electronic privacy policies and consent directives. The contents and semantics are standardized by two recent specifications that include US-based requirements for privacy policy and consent directives:

1. Composite Privacy Consent Directive DSTU – a standard model to describe electronic/interoperable Privacy Policies and Consent Directives. This standard was developed in collaboration with Security WG.
2. Consent Directive Clinical Document Architecture (CDA) Implementation Guide - a document exchange standard based on the Composite Privacy Consent Directive DSTU. This standard was developed in collaboration with Security WG.

Note: These two specifications are referred collectively as the "Composite Privacy standards" for the rest of this document.

Previously approved specifications ("Data Consent Version 1.0") have been adopted successfully in Canada. The approval of the Composite Privacy standards introduced support for US-based privacy policies and privacy consent directives to support PHRs, nation wide health information exchange, and empower consumers. These Composite Privacy standards specify the common contextual attributes of health information that determine which health information is deemed "sensitive" in the context of a specific privacy policy. Contextual information such as the diagnosis/problem (e.g. substance abuse, mental health), the payment method (e.g. cash payments), the type of information (e.g. genomics), the insurance program (e.g. private vs. public insurance, Medicaid) is explicitly stated in privacy policies. The specifications empowers consumers by standardizing active consent choices to share or not share information based on consumer's own decisions thus enabling more control and choice for consumers in control of their healthcare data.

Composite Privacy Standards

Consistent Representation of Privacy Policies and Consent Directives

The Composite Privacy Consent standards are based on the premise that more than one privacy policy may be applicable in any organization. HIPAA Privacy provides the floor, or baseline protection on which other policies are layered (e.g. Genetic Information Non-Discrimination Act of 2008- GINA, Confidentiality of Alcohol and Drug Abuse Patient Records – 42 CFR Part 2, ARRA HITECH Act Cash Payments, state law for HIV and Sexually Transmitted Disease (STD), state law regarding the confidentiality provided to Medicaid patients and other vulnerable populations). The Composite Privacy standards

define the common elements across all these policies in a standard-based and interoperable form that is implementation neutral. Therefore whether the standard is used to author privacy policies or privacy consent directives, the criteria used to specify sensitive information will be consistent across policies and privacy consents.

Analysis and reconciliation based on common privacy criteria

The HL7 Composite Privacy standards allows healthcare providers to automatically delineate sensitive information including contextual criteria specified by a privacy policy and/or privacy consent directive based on a standard set criteria. The consistent privacy criteria specified by Composite Privacy standards enables both analysis and reconciliation of different policies based the standard set of criteria (e.g. information type, related diagnosis, population type, payment method) regardless of implementation. For example if a state policy specifies mental health information is sensitive and a separate policy exists to protect the privacy of Medicaid patients extending sensitivity to HIV and Sexually Transmitted Disease information, then if these policies were available in a standard form, the policies could be automatically analyzed and the resulting reconciled policy would deem that a Medicaid patient's mental health, HIV, and STD information are all sensitive and thus will not be exchanged with other organizations without the patient consent.

Support for a variety of computer security technologies

Simply by describing privacy policies and privacy consent directives using standard-based, computable criteria HL7 Composite Privacy standards enable computer systems and business rules engines to distinguish sensitive data and manage it appropriately. Furthermore, these standards promote the adoption of established technology approaches (e.g. access control, digital rights) to manage sensitive healthcare information by bridging the gap between the health information representation and the privacy policies that apply. The ability to represent privacy policies and privacy consent directives in electronic and interoperable form is especially important when policies have to be compared and reconciled across jurisdictions. It is also beneficial to have a direct and computable link between the policy and the information exchanged between healthcare providers across a nationwide network or served directly from a Personal Health Record (PHR) to providers or research and marketing purposes by allowing patients to specify complex criteria describing the type of information that should be protected. This empowers patients/consumers and ensures trust in the overall privacy of interconnected information systems.

A comprehensive approach to privacy

The Composite Privacy Consent standards are based on the premise that more than one privacy policy may be applicable in any organization: HIPAA Privacy provides the floor, or baseline protection on which other policies are layered (e.g. Genetic Information Non-Discrimination Act of 2008- GINA, Confidentiality of Alcohol and Drug Abuse Patient Records – 42 CFR Part 2, ARRA HITECH Act Cash Payments, state law re: HIV, STD,

state law regarding the confidentiality Medicaid patients). The Composite Privacy standards define the common elements across all these policies in a standard and interoperable form that is implementation neutral.

Future Work

The CBCC WG recently approved a new Semantic Health Information Performance and Privacy Standard (SHIPPS) project intended to identify and define the metadata and data quality (structured encoded data) necessary to:

1. Segment and manage sensitive health information (in support of privacy protection) and
2. Enable real-time performance evaluation: the ability to automate the use of EHR systems data for the purposes of quality outcomes measurement and performance

It is important that healthcare providers invest in information systems (e.g. Electronic Health Record Systems) that are able to create structured and standard-encoded information ready to be processed for a variety of purposes (e.g. to identify sensitive information according to a specific policy, to compute real-time quality measures).

Security Work Group has developed a Harmonized Security and Privacy Model to address both the policy and implementation viewpoints. This specification is undergoing final revisions before it will be published as a Draft Standard for Trial Use.

Confidentiality Attributes and Confidentiality Code System

HL7 specifies that information artifacts represented using the HL7 Reference Information Model may include a confidentiality attribute intended to specify whether an information object is sensitive or not. For example a clinical document may be deemed sensitive if its content is identified by a specific privacy policy. Sensitivity is an intrinsic property of an information artifact and it is determined based on privacy policies. The confidentiality attribute may be added to the information exchange envelope to specify how participants in an information exchange should handle information intended to be protected based on privacy policy. For example, sensitive information may have to be encrypted and its content must be secured against tampering during transport.

Terminology Issues and Recommendations

Currently the “confidentialityCode” attribute specified in the HL7 Reference Information Model (RIM) is ambiguous as it attempts to specify both the sensitivity of health information and how that health information may be accessed by users. According to the HL7 RIM, the definition of the confidentiality code “needs work in particular to help distinguish and identify the relationship between the types of concepts that it conveys and how best to encode and communicate them with this one attribute.” Therefore, implementers should use the confidentiality code as the single basis of determining if information is sensitive, and it is a useful means of conveying that the data is protected

by policy. In other words, an information object is marked as sensitive using confidentiality code only after the system determines that its content is intended to be protected according to privacy policies (e.g. sensitive diagnosis, vulnerable population, self/cash pay for services). Clearly this level of automation is only possible with structured and standard-encoded information.

Confidentiality codes for information exchange

It is conceivable and desirable to rely on confidentiality codes while health information is in transit and triggers specific security mechanisms (e.g. transport level security – encryption) for sensitive information that may not be needed for routine (non-sensitive) information. Therefore, as a matter of best practice from a privacy stand-point, implementers of EHRS and PHR system should avoid the HL7 ConfidentialityByInfoType value set specified in the Confidentiality [2.16.840.1.113883.1.11.10228] code system for the following reasons:

1. It was not intended to be used with identifiable/actual patient data (as specified in the definition of the value set).
2. The codes HIV-for HIV related, ETH-for Substance Abuse related, PSY-for psychiatry related, and SDV-for Sexual and domestic violence related would reveal too much of the nature of the sensitive information intended to be protected. If this code is used in a transport envelope or clinical document registry it would inadvertently disclose information to unauthorized users. It would be preferable that data related to sensitive conditions simply be marked sensitive without specifying the condition.
3. These codes are used as short-hand to reference the privacy policy dealing with certain conditions or problems. Enumerating these policies in a code set is not scalable as new privacy policies are introduced overtime. In the US this value set would have to be extended to include sickle cell anemia and sexually transmitted diseases and it would have to be continuously updated as new policies are added.

Another HL7 Confidentiality value set that requires careful consideration is the ConfidentialityByAccessKind value set, as some of its values explicitly do not allow for use with identifiable/actual patient data and implementers may assign them erroneously. This value set should be refactored to separate codes that are applicable to patient information from those that only apply to other types of information. It is also specific to some "service" – presumably a medical service delivered to a consumer.

1. Some codes in this value set refer not to an intrinsic sensitivity of the information object but to an external policy. Therefore this would be better addressed as a reference to that uniquely identified policy rather than a code:
    - "D" specifies that "only clinicians may see this item".
    - "I" specifies that the information system may allow access "only to individual persons who are mentioned explicitly as actors of this service and whose actor type warrants that access (cf. to actor type code)."
2. Some codes are explicitly not allowed for patient information

    - “B” refers to “business secret” and should not be used for patient information: “However, no patient related information may ever be of this confidentiality level.”
    - ”L” – low confidentiality code – is explicitly prohibited for patient information: "No patient record item can be of low confidentiality. However, some service objects are not patient related and therefore may have low confidentiality.”
3. As it stands today, this value set represents an incomplete list of “hardcoded” access control policies limiting access to information based on a broad category of structural and functional user roles. These policies could be implemented very differently.

Appendix B

HL7 and the HL7 Personal Health Record System Functional Model (PHR-S-FM)

HL7

Established in 1987, Health Level Seven International (HL7) is an American National Standards Institute (ANSI) accredited, not-for-profit standards-development organization, whose mission is to provide standards for the exchange, integration, sharing, and retrieval of electronic health information; support clinical practice; and support the management, delivery and evaluation of health services. ANSI accreditation, coupled with HL7's own procedures, dictates that any standard published by HL7 and submitted to ANSI for approval, be developed and ratified by a process that adheres to ANSI's procedures for open consensus and meets a balance of interest requirement by attaining near equal participation in the voting process by the various constituencies that are materially affected by the standard (e.g., vendors, providers, government agencies, consultants, non-profit organizations, etc.). This ANSI required balance of interest goal ensures that a particular constituency is neither refused participation nor is it allowed to dominate the development and ratification of a proposed standard.

The PHR-S-FM

The HL7 Personal Health Record System Functional Model (PHR-S FM) was first released for public comment in August 2007. In November, 2007 the Draft Standard for Trail Use (DSTU) version of the PHR-S FM was released for comment. The comments received where then incorporated into the current July 2008 DSTU which is now completing a period for general review and Trial Use from the entire HL7 organization. This current PHR-S-FM DSTU is now nearing completion and preparation is already underway by the WG to use the knowledge gained in this trial process to complete a balloted version that will be published as both an HL7 and ISO TC215 (International Standards Organization Medical Informatics Technical Committee) normative standards. The PHR WG makes a clear distinction between a Personal Health Record (PHR) and a PHR System (PHR-S). The PHR is the underlying record that the software functionality of a PHR System maintains. There has been much discussion surrounding the definition of a personal health record. The PHR-S FM does not attempt to define the PHR, but rather identify the features and functions in a system necessary to create and effectively manage PHRs.

The overarching theme of a PHR-S involves a patient-centric tool that is controlled, for the most part, by the individual. A PHR-S should be immediately available electronically and able to link to other systems. The PHR-S is intended to provide functionality to help an individual maintain a longitudinal view of his or her health history, and may be comprised of information from a plethora of sources – e.g., from providers and health

plans, as well as from the individual. Data collected by the system is administrative and/or clinical, and the tool may provide access to a wealth of health-related forms (e.g., Advance Directives) and advice (e.g., diet, exercise, or disease management). A PHR-S might also help the individual collect behavioral health, public health, patient-entered and patient-accessed data (including medical monitoring devices), medication information, care management plans and the like, and might be connected to providers, laboratories, pharmacies, nursing homes, hospitals and other institutions and clinical resources.
At its core, the PHR-S should provide the ability for the individual to capture and maintain demographic, insurance coverage, and provider information. It should also provide the ability to capture health history in the form of a health summary, problems, conditions, symptoms, allergies, medications, laboratory and other test results, immunizations and encounters. Additionally, personal care planning features such as Advance Directives and care plans should be available. The system must be secure and have appropriate identity and access management capabilities, and must use standard nomenclature, coding and data exchange standards for consistency and interoperability. A host of optional features have been addressed over the course of this initiative, including secure messaging, graphical presentation of test results, patient education, guideline-based reminders, appointment scheduling and reminders, drug-drug interactions, formulary management, health care cost comparisons, document storage and clinical trial eligibility.

The effective use of a PHR-S is a key point for improving healthcare in terms of self-management, patient-provider communication and quality outcomes.

The HL7 PHR-S FM defines a standardized model of the functions that may be present in PHR Systems.

This PHR-S-FM is not:

- A messaging specification
- An implementation specification
- A conformance specification
- A specification for the underlying PHR (i.e., the record itself)
- An exercise in creating a definition for a PHR
- A conformance or conformance testing metric
- A requirement specification for a single PHR
- An architecture specification for a PHR-S
- A substitute for policy governing the function, availability or use of a PHR-S.

The information exchange enabled by the PHR-S supports the retrieval and population of clinical documents, event summaries, minimum data sets, claims attachments, and in the future will enable a longitudinal health record.