Comments —NBP Public Notice # 29
Referencing GN Docket Nos. 09-47, 09-51, and 09-137

Introduction: Assuming Privacy

My organization (www.tolven.org) has created software that assumes that patient privacy and protection of healthcare information is essential for widespread adoption of a nationwide network of health information creation and exchange. We firmly believe that any distribution of health care information outside of the organization that created it must be under the control of the patient unless such distribution is mandated by government regulation (such as for public health reporting for critical exercises in epidemiology).

Technical empowerment of principles of patient privacy is not only feasible and practical, it is taking place today. In the following sections, I shall review features of "security by design "as we have understood and implemented it with our partners.

Security by Design: Articulating Principles (Health Record Banking Alliance)

The Health Record Banking Alliance (www.healthbanking.org) has published a set of principles that include recommendations for protecting the privacy of personal health care information.

HRBA Principles

Consumer Ownership and Control of Health Records

1. Health record banks protect the individual consumer's right to health information privacy and confidentiality by acting as trusted legal custodians of consumers' health records.

2. Health record banks are repositories for trustworthy copies of health information selected or submitted by the consumer from various sources.

3. Health information in a health record bank is owned by the consumer and is not an asset of the health record bank.

4. Consumers may authorize someone else to manage their health record bank account.

5. Health record banks provide consumers and others they authorize with immediate electronic access to their health information.

6. Consumers control all disclosures of their health information by a health record bank unless otherwise required by law.

7. With consumer consent based on advance disclosure appropriate to the circumstances, health record banks enable secondary use of health information, such as for public health and research purposes.

Operation of Health Record Banks

8. Health record banks are governed in an open, accountable, and transparent manner.

9. All access and updates to information in health record banks are recorded as they occur in an appropriately detailed audit trail database, and each health record bank shall maintain those unaltered audit records at least during the time that a consumer's health record is kept at the bank and make those audit records immediately accessible to consumers.

10. Health record banks have established processes for correcting errors by updating, amending, and sequestering data, including mechanisms for notification of parties who have received such data.

11. Health record banks promptly disclose breaches of privacy, confidentiality, or security to consumers.

Operation of the HRBA

12. The HRBA seeks to maintain neutrality among vendors that agree to adhere to the above principles.

Definitions used by the HRBA in its statement of principles.
Derived from a letter from the National Committee on Vital and Health Statistics to Secretary of HHS sent to Michael Leavitt, 6/22/06.

Health information privacy refers to an individual's right to control the acquisition, use, or disclosure of his or her identifiable health data.

Confidentiality refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

Security refers to the physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

Security by Design: an Implementation in the Netherlands (Stichting Rijnmondnet)

A project in the Netherlands managed by Stichting Rijnmond (http://www.rijnmondnet.nl/) adheres to the principles outlined by the Health Record Banking Alliance. In this project, the patient controls the distribution of his/her personal healthcare information.

Stichting Rijnmond is implementing a patient-centered system for exchange of health information between hospitals, patients, and physician offices in the Netherlands. In this implementation, patient participation is required for any exchange of information across stakeholder boundaries. The functional outline of the system follows.

1. Clinical information is packaged in conformity with the HL7 CDA standard before it is sent from the medical center to a "holding area" repository, which we can call the Medical Center electronic Clinical Health Record (MC eCHR).
    a. All information sent to the MC eCHR will be contained in CDA documents that contain the patient's BSN (a unique coded identifier issued by the government)
    b. No patient can view information in the MC eCHR
        i. A patient is only able to view their own clinical information when copies of that information have been sent to the patient's ePHR from the MC eCHR
    c. No clinician can view information in the MC eCHR
        i. A clinician is only able to view copies of that information that have been sent by a patient from a patient ePHR to either a Clinician eCHR or a Specialty eCHR
2. Each participating clinician has his/her own Clinician eCHR account
    a. There is only one clinician for each Clinician eCHR account and only one Clinician eCHR account for any clinician
3. Each participating clinician can also be a member of a specialty account which has its own Specialty eCHR
    a. Any clinician can have one Clinician eCHR and be a member of one Specialty eCHR
    b. A Specialty eCHR account contains no clinical information until copies of clinical information are sent to it from one or more ePHRs
    c. Each member of a Specialty eCHR account is able to view information that has been copied to that Specialty eCHR
    d. Specialty eCHR account set up and membership is controlled by administrative staff under the guidance of Stichting Rijnmond
4. Any participating patient has the opportunity to create an ePHR account
    a. When the patient first logs into the system site, the action references that patient user's BSN
    b. A secure exchange between the patient and the system results in the set up of the ePHR account
    c. This patient user must log into his ePHR account and create a "patient" (himself) using the appropriate application screens
    d. The ePHR patient user can now browse the list of clinical organizations that participate in the project
    e. The patient user can now select the appropriate medical center in order to receive copies of his/her information from the MC eCHR account
        i. If the patient user fails to perform this step, there will be no clinical information in his ePHR

    f. Upon receipt (and approval) of the request by the MC eCHR, all CDA documents for that patient (identified by the BSN) from that time forward will be automatically copied from the MC eCHR and sent to that patient's ePHR. This process is automated and does not require any human interaction.
        i. All document copies sent to the ePHR are processed according to system rules so that presentation of information is easily navigable by the users
        ii. At any time, the patient may cease participation
    g. The ePHR user can now browse the list of participating clinical organizations, which includes the individual clinicians participating in the pilot as well as the Specialty groups participating in the pilot
    h. There is an hierarchical selection list allowing for the desired functionality of selecting providers via navigation through Specialty groups
        i. The patient user can now select which Clinician eCHR or which Specialty eCHR account can receive copies from this ePHR
            1. This process can be repeated to identify additional account recipients
    i. In his/her ePHR, the patient user can navigate to the "share" function and select the provider to receive copies of clinical information from this ePHR
        i. The ePHR user now can select any or all categories of information to be copied to the selected "provider"
        ii. The patient may take action to have this flow of information cease at any time
5. A participating clinician has a Clinician eCHR account created for him by an authorized medical center/Stichting Rijnmond administrator
    a. That account contains no clinical information until copies of clinical information are sent to it from one or more ePHRs
    b. This clinician must create himself as a "provider" by using the appropriate application screens
        i. Submitting this information places this clinician's name on the "Public" provider list allowing for viewing by patients in the system
        ii. Additional application functionality allows for selection of providers via navigation through Specialty group
6. An authorized clinician/administrator of a Specialty group navigates to the appropriate medical center/Stichting Rijnmond web site to create a Specialty eCHR account
    a. The first step is to register a new user (unless this authorized clinician/administrator is already an authorized system user)
        i. Once this step is completed, user activation (via secure email exchange containing encrypted url) takes place
    b. The activated user now creates a Specialty eCHR account
        i. This user should only create one Specialty eCHR account for any Specialty group
        ii. That account contains no clinical information until copies of clinical information are sent to it from one or more ePHRs

        iii. The authorized clinician/administrator uses the appropriate application screens to add additional users for this Specialty eCHR account
            1. This assumes that all of the "additional users" have already "created themselves" following the steps in #5 above
    c. The clinician/administrator must create a Specialty "provider" group by using appropriate application screens
        i. This action places this Specialty Group's name on the "Public" provider list for viewing by patients in the system
7. A patient can send copies of any documents held in his/her ePHR account to any Clinician eCHR whose clinician name appears on the "public" Provider list
    a. CDA document copies sent to any Clinician eCHR will appear on that account's "Inbox"
    b. When the Clinician eCHR user "opens" any item on the "Inbox" list and "Submits" it, that item is removed from the Inbox list and is then processed according to current system rules for easy navigation and viewing
8. A patient can send copies of any documents held in his ePHR account to any Specialty eCHR whose group name appears on the "public" Provider list
    a. CDA document copies sent to any Specialty eCHR will appear on that account's "Inbox" list
    b. When the Specialty eCHR user "opens" any item on the "Inbox" list and "Submits" it, that item is removed from the Inbox list and is then processed according to current system rules for easy navigation and viewing

Security by Design: Technical Infrastructure (Tolven)

The Tolven open source platform and application development environment is being used by a number of electronic healthcare information projects being implemented by Tolven and its partners (http://www.tolvenhealth.com/TolvenClients.html), among them the Stichting Rijnmond project. Tolven based systems are web based allowing for broad participation by authorized users. The following comments regarding security and privacy are derived from documents available on the Tolven web site (http://www.tolven.org/architecture/briefs/index.html)

1. The Tolven platform and applications approach the issue of "consent" by including provisions for the following:
    a. Consumers have the right to opt out of participating at any time
    b. Once consumers have elected to "opt in" they can also explicitly grant consent to authorized users to view only specified sections of their personal healthcare information
    c. Consent to view/not view can be limited to selected logically meaningful categories of information in their medical records
    d. Consent may be granted (or denied) to individuals or groups
    e. The pairing of the Tolven eCHR and the Tolven ePHR empowers consumers and their families/agents to participate in managing their healthcare to an extent not yet seen because each can easily exchange information with the other, upon registration of consent.

2. Tolven is concerned with protecting data in transit (eg SSL) and protecting data at rest (e.g. in the database).
    a. Tolven requires proper authentication of users, accounts (e.g. family, clinic, lab, etc), and system components (App server, LDAP server, Database server).

3. End users (via their browser) verify authenticity of Web/application server using digital certificates.
    a. SSL then protects the communication between browser and application server from "man in the middle" attack.
    b. The application server, with the aide of the LDAP server, usually authenticates the user via username and password entry.
    c. This accounts for the bulk of the visible web-based security most people see.

4. Although typically behind a firewall, Tolven further requires mutual authentication (digital certificates) and secure communication (SSL/TLS) between backend system components.
    a. For example, the application server must authenticate the database server that it connects to and likewise the database server must authenticate the application server.
    b. The same approach is used for communication between the application server and the LDAP server.

5. While SSL is designed to guard against "man in the middle" attacks, it does nothing to protect data once it arrives at its destination where the SSL encryption is removed.
    a. In Tolven, new document data is immediately encrypted in the application server, before being transported to the database.
    b. Thus, as a new document travels from the application server to the database server, it is essentially double encrypted because of SSL.
    c. Upon arrival, the SSL encryption is removed.
    d. Yet, when the document comes to rest, it is still encrypted because of the document-level encryption.

6. Document encryption provides an "absolute" level of protection between Tolven accounts.
    a. For example, a document created, say, in a person's personal health record is only visible to users of that personal health record account, typically that one person or members of that person's family. No one else.
    b. This absolute partition cannot be violated, even by a system administrator with root passwords and a complete copy of the (encrypted) data, log files, etc.

    c. It would be as unusual for a physician to have access to someone's personal account as it would for a patient to have access to data in the physician's account.

7. The process of sharing data between accounts in Tolven is explicit.
    a. Simply granting users in one account access to see data in another account is not allowed and if it were, it wouldn't do any good because of the "absolute" encryption described above.
    b. Instead, to share data between accounts requires a user in the outgoing account to initiate an action that internally makes a *copy* of the source document encrypted so that only members of the receiving account can read the *copy*.
    c. This is why we say "Privacy is enhanced at the cost of extra disk space" This explicit action provides a very reliable audit trail because the act of sharing data is recorded in space and time with the medium being the document itself.
    d. If a citizen *opts in* to a research program, cancer registry, public health, shares an intake questionnaire (clip board) with his or her family doctor or a physician releases a lab result to the patient, each such sharing is explicitly recorded in the form of a new document only visible to members of the receiving account.

8. Sharing data among users within a single account is not subject to such strict control as above.
    a. When needed, access can be controlled by "traditional" authorization, role-based access.
    b. However, Tolven expects accounts to be small enough (a family or a single clinic for example) so that cumbersome user-level permission schemes can be reduced or avoided completely.

9. SSL, TLS, X.509, PKCS, WS-Security, etc are protocols and wrappers around the actual low-level encryption and public/private key algorithms.
    a. The algorithms (RSA, DES, 3DES, AES, etc) and corresponding strengths or key lengths evolve over time as CPU speeds increase.
    b. In order to avoid a lock-in to specific algorithms, Tolven uses the openSSL framework for SSL and the JCE framework for document encryption so that as new algorithms are added or specific countries impose restrictions, only parametric changes are required.

10. Security standards are particularly important for data at rest since encrypted documents may exist for decades.
    a. It would impractical to re-encrypt existing documents; so, many different encryption techniques may be in use over time.

11. Digital signatures of documents in Tolven is somewhat related to encryption because many of the underlying algorithms are the same.

a. While documents are encrypted at the account level, signatures on a document are attributed to individual users.
b. A document can be signed by one or more users.
c. A copied document, as long as it has not been changed from the original, can retain its signatures even if it moves to an account where that user is not a member.
d. For example, if a physician "signs" a lab result and then sends the result (a copy actually) to the patient, the physician's signature is retained.
e. The consumer or even a privileged system administrator (or someone else in the middle) would not be able to modify or counterfeit a document without invalidating the signature.

Thomas M Jones, MD
Chief Medical Officer, Tolven Inc. 18955 Viewcrest Drive
Sonoma, CA 95476

tom.jones@tolvenhealth.com

707 695 5712 (mobile)
707 939 7845 (office)