PPR Framework for Patient ID

Adrian Gropper MD, CTO, Patient Privacy Rights

May 2013

1 - Abstract

Patient ID is now the focus of federal, state and private efforts for health information exchange because it is a limiting factor in health communications. Patient Privacy Rights is developing a robust and privacy-preserving framework for Patient ID based on widely accepted fair information practices. PPR is seeking collaborators to implement and pilot the PPR Patient ID Framework.

Fair information practices require services to:

- minimize their request for private information,
- minimize the information sent to other services, and
- provide transparency.

The PPR Patient ID Framework applies these principles by defining three levels of health ID application:

1. isolated services,
2. associated services, and
3. aggregated services.

The PPR Framework for Patient ID focuses on level 3 - aggregated services and suggests best practices for deploying Patient ID based on routable, voluntary, globally unique identifiers and a standardized Patient ID Notice of Privacy Practices. All aspects of the Framework are non-proprietary and based on well-established Internet practices.

The sharing and aggregation of health data is essential for safe and cost-effective care for the individual and for medical progress that benefits us all. Conversely, lack of trust and risk of discrimination causes patients to delay treatment or withhold information essential for public health. Patient ID practices that promote trust and provide full transparency to the patient will increase both the quantity and the quality of medical data available for both treatment and research.

For patients, the Framework uses concepts as familiar as email and the W9 new employee registration form to enable patients to understand the implications of their identity-related decisions.

For providers, the Framework requires minimal retooling of existing systems because it impacts only the external interfaces of the institutional system while leaving internal medical record numbers and interfaces to payors and other directly associated systems unchanged.

For health information exchanges and registries, the Framework provides the essential index to which consent management, record locator services and accounting for disclosures can be linked while reducing the costs and risks associated with master patient index approaches.

2 - Patient ID Problems

Patient ID problems result in unintended or unlawful disclosure of a patient's information. The nature of the information disclosed can be as simple as a visit to a mental health provider or a clinic associated with a particular specialty. The actual content or result of the visit need not be divulged in order to violate a person's privacy - documentation that the visit took place is often more than the person is willing to share or add to one's aggregated health record. Once a visit is documented, the person is exposed to inquiry as to the reason for the visit from prospective employers, insurance companies and even family members.

Celebrities and VIPs guard their privacy by hiding their identity behind pseudonyms. This adds complexity and cost to their service relationships and can have unintended personal safety issues as errors and fragmentation creep into their health records. Strict pseudonymity for every patient would make our healthcare system more expensive and less reliable and would hinder both research and public health.

Patient ID and information disclosure beyond the strict control of an institution can be limited by law and by self-attested policy. Any personally identifiable information that leaves the control of an institution intentionally should be identified unambiguously to provide accountability and facilitate downstream uses. All other sharing of personally identifiable information would be considered a breach under HIPAA, FTC or other regulations.

Patient ID problems include ambiguity, coercion and usability.

Problems arise when the patient ID associated with information is ambiguous. For example, a simple name and address does not account for people that have moved and can have a surprisingly high failure rate with foreign names and as a result of encoding issues. Mis-spelling or transcription errors can also be a problem. With the advent of ubiquitous connectivity via Internet and cellular service, the problem of ambiguous ID can be eliminated by using routable identifiers whose accuracy can be verified in seconds by simply sending a text or email message with a confirmation response.

Coercion problems arise when patient ID becomes a tool for involuntary surveillance and tracking beyond the control of the person. The right to seek medical care privately and even anonymously is essential and should not be denied by requiring federally issued and biometric IDs in routine clinical encounters. Only in very special cases such as narcotic drug prescription registries and mental health background checks for gun purchase should a patient be forced to use a coercive ID. Even in these extreme cases, a patient should know that a coercive ID is in use so that they can refuse the service and track errors that might creep into the surveillance system. Unlike law enforcement, there is no role for secret surveillance in healthcare.

Usability problems arise when the patient ID is costly to administer or incompatible with typical activities. The use of driver's license numbers is a problem for minors and foreigners. Social security numbers is a problem for identity theft. The use of smart cards is a cost and infrastructure problem. Proprietary systems such as VUHID depend on the policies and stability of new and untested business.

Because Patient ID is a fundamental commodity, governance and regulatory issues can also lead to problems. Legal prohibitions against a coercive federal ID system and a reluctance of states to take on added service responsibilities means that private-sector solutions need to be effectively regulated. Private-sector ID services need to be fair, sustainable and responsive to changes in both technology and culture. Both public and private patient ID systems need a very high level of transparency and accountability to promote trust and to avoid conflict of interest and commercial abuse.

Patient ID problems also contribute to many other privacy harms and systems costs. Data segmentation, the legal mandate to separate out mental health, substance abuse, and select other segments of a health record, is made much more difficult if all of the segments are labeled with the same Patient ID. The availability of multiple, voluntary, patient-friendly Patient IDs makes segmentation much easier because it allows the patient to see and correct any problems.

Without a robust Patient ID infrastructure, consent, password management and family caregiving are all much less convenient for the patient. A consent management system that is not tied to specific and transparent patient ID is difficult for the patient to understand because their information is scattered among any number of institutions. A Patient ID system that does not support single-sign-on technology forces patients to create and keep track of separate user IDs and passwords for every service provider's portal. A Patient ID system that does not allow for delegation of authority to a health care proxy makes family caregiving much more complex and introduces major security vulnerabilities as passwords become routinely shared among different people.

A thorough discussion of Patient ID problems is well beyond the scope of this paper. Here's a short bibliography of relevant projects:

- Federal prohibition on issuing a national ID (need reference)
- RealID controversy (need reference)
- ONC NwHIN Governance Use Existing levers and Guidance
    - Lead Through Action:Use available levers to directly accomplish specific goals
    - Lead through Guidance : Disseminate a framework of principles and, where available, good practices, models, and tools for specific exchange challenges
    - Engage, Listen, and Learn: Proactively encourage and engage with communities and stakeholders offering solutions for exchange.
    - Monitor: Monitor marketplace for abuses, exchange successes, gaps and failures; and consumer and provider attitudes
- Record locator services for state HIE Mass HIway NYeC
- National Instant Criminal Background Check System
- CommonWell Health Alliance
- NSTIC / IDESG Healthcare Subgroup
- DirectTrust.org

3 - Fair Information Practices

The Fair Information Practice Principles (http://www.nist.gov/nstic/NSTIC-FIPPs.pdf)

To truly enhance privacy in the conduct of online transactions, Fair Information Practice Principles (FIPPs) must be universally and consistently adopted and applied in the Identity Ecosystem. FIPPs are the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.1
In brief, the Fair Information Practice Principles are:

- **Transparency**: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).
- **Individual Participation**: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
- **Purpose Specification**: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to

be used.

- **Data Minimization**: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- **Use Limitation**: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity**: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- **Security**: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Universal application of FIPPs provides the basis for confidence and trust in online transactions.

<end of NSTIC citation>

Other perspectives on personal ID include Kim Cameron - 7 Laws of Identity; FTC; EU Data Protection Directive; HIPAA Omnibus Rule in Federal Register (Need reference to information minimization), and OCR Blue Button Plus Security and Privacy Guidance.

Although all of the principles are important, for the purposes of the PPR Framework for Patient ID, we choose to focus on three principles in particular:

1. Data minimization when registering for a new healthcare service
2. Data minimization when a health care service shares ID information externally
3. Transparency to the patient of what ID will be used for surveillance and aggregation

An example of Principle 1 would be that a lab that is to perform a blood test should accept any patient ID as long as the ID is guaranteed to return the result to the patient that gave the blood sample. This would allow for anonymous or pseudonymous ID as long as the ID could be verifiably linked to a patient’s ability to receive the result message.

An example of Principle 2 would be that external communication of the blood test service to a record locator service would be unambiguously tagged with a globally unique patient identifier as supplied by the patient. The use of an anonymous or pseudonymous ID is allowed as long as the patient can prove that they control that ID in order to avoid errors and malicious spam of other people’s records.

An example of Principle 3 is to ensure that the patient knows how their health care service will be indexed and can easily and conveniently check that it was indexed correctly. This can be achieved by linking the ID to a well-known on-line registry that the patient can access conveniently, securely and without charge.

4 - Three Service Levels

Patient registration is the seminal event of a patient’s interaction with a clinical service provider. The PPR Framework for Patient ID is designed to apply fair information practices to the patient registration process while taking advantage of current technology.

In the paper world, patient registration is represented by the clipboard and a multi-page HIPAA Notice of Privacy Practices. It is often accompanied by the imaging of the patient's Driver's License and Health Insurance Card. No aspect of this process is standardized and very little of it is patient-friendly.

The PPR Framework for Patient ID is not limited to paper or to any particular level of healthcare service. It's designed to allow paperless implementation, if available and to span all healthcare services from the most trivial to the most serious. At one end of the spectrum we might have the purchase of an over-the-counter diagnostic test at the local pharmacy. At the other end, we might have a visit with a psychiatrist.

The Framework categorizes three levels of health services encounters: isolated, associated and aggregated.

Level 1: Isolated - An isolated encounter is a simple consultation between a physician and a patient, a laboratory procedure or the purchase of an over-the-counter drug. If a simple encounter is paid in cash, the only reason to have any persistent Patient ID is to allow for on-line patient access to the records and for aggregation of a health record over time with the service provider. Patients have a right to anonymous care so the number of patients that actually seek to exercise that right is irrelevant.

An isolated encounter, by definition, involves only one legal entity and does not send any information beyond the service provider's systems and, as such, has relatively few privacy implications. The Notice of Privacy Practices for an isolated encounter can be very simple and state in plain language that no information will be sent anywhere for any reason with first notifying and possibly seeking specific authorization by the patient.

A simple picture of the patient at registration associated with an ID number specific to the practice could be all that's required. The patient might also be allowed to choose a password for on-line access or to present a public key for secure messaging compatible with the Direct project standards. (http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport)

Level 2: Associated - An isolated encounter becomes an associated encounter when a second legal entity is involved. Typically, this is a result of insurance payments or prescription fulfillment. An isolated encounter does not give either of the two service providers in the association the right to send information about the encounter beyond their systems. The Notice of Privacy Practices for an associated encounter can list the specific legal entities by name and state clearly that neither entity has any right to share information without first notifying the patient and possibly seeking specific authorization. Patients can expect that information to be shared as part of an association such as provider-to-payer or provider -to-pharmacy does not automatically extend to use of that information in any other context such as aggregation, health information exchange or research.

Any patient ID that is unambiguously known to both parties to an associated encounter is all that's needed. This is typically the insurance plan number or, in the case of a prescription, a provider's internal medical record number.

For added privacy, the patient ID on a prescription should be specific to that prescription to avoid the unintended surveillance. It should be noted that today's e-prescribing systems do not provide this level of privacy protection. This causes problems with data segmentation as required by law for health care encounters that are paid in cash.

Level 3: Aggregated - An aggregated health service encounter provides a means of surveillance and information aggregation for the benefit of the patient and public health. Examples of information aggregation include:

- listing of the encounter in a state health record locator service
- posting of the encounter on a state All Payer Claims Database
- sending information to a state Immunization Registry
- sending information to a PHR such as Microsoft HealthVault
- submission to a research, clinical trials or disease tracking registry
- sending information to a state Prescription Drug Monitoring Program
- sending information to a state Firearms Purchase Registry

All of the aggregated examples share the risk of unintended consequences and difficulty in correcting errors. Many expose the patient to risks in securing employment or insurance. Some, like the ones involving genetic data, may impact family members. Others, like parental decisions on behalf of minor children can impact the adult.

None of the aggregated examples above are cause for secret or hidden surveillance. Patients need to be able to conveniently access all of the information aggregated on their behalf.

Prescription drug monitoring and firearms mental health registries are the only examples above that require a coercive or involuntary ID to prevent duplicate accounts. In all other cases, fair information practices suggest that the patient be allowed to voluntarily segment health service encounters by perceived sensitivity or purpose.

The Notice of Privacy Practices associated with a patient registration event that seeks to aggregate information can be designed according to fair information practice principles. If the Notice provided at registration is inadequate for information aggregation, the service provider can choose to request specific patient authorization or can provide a new Notice of Privacy Practices for patient approval.

Fair information practices during the patient registration process require data minimization and transparency appropriate to the service level the patient expects and any escalation of data use privilege should be done without coercion and with informed consent.

A user-friendly registration experience will develop trust and encourage the patient to allow data aggregation for patient safety, research and public health. The registration experience should include some or all of the following features in order to improve patient engagement and data reuse:

- A Routable ID - An ID is routable if it can be used to send a message to the patient. Examples include cell phone numbers and email addresses. A routable ID is guaranteed to be unique to avoid errors due to duplicated users, can eliminate keyboarding errors, provide the patient with a permanent record of their registration and avoid more intrusive identity verification requests. A routable ID is also more likely to be remembered by the patient so it reduces the inadvertent creation of multiple identities and the resulting involuntary fragmentation of the aggregated health record.

- Separation of ID from Certifications - An ID that is independent of any particular affiliation, certification or role is more likely to persist over time and to provide a higher quality of user experience. Participation in a particular insurance plan or a place of employment is typically temporary and may be beyond the patient's control. As with phone number portability, the patient's interests are best preserved when they are in control of their identity. Affiliation and certification can be securely attached to a patient ID through technical means.

- Serving the oblivious and underprivileged - Patients should not be expected to remember too much as part of a registration event. If possible, the Notice of Privacy Practices should be pre-filled with patient name and contact information if that is known to the practice as a result of a referral or an appointment process. To avoid coercion, the patient should be allowed to erase or modify any pre-filled information. To promote usability, the patient can be allowed to sign-in to an independent ID provider such as Open ID Connect to transfer information that populates the registration form.

- Avoiding secret surveillance - The Notice of Privacy Practices should clearly tell people all of the places that will aggregate their information and provide log-in information so that they can periodically check its accuracy.

- Facilitating accounting for disclosures - The Notice of Privacy Practices should include clear indication of how the patient can see an up-to-date list of all information disclosures by the service provider. This list should be transparent by including a link for the patient to see the actual information that was shared.

- Open, non-proprietary, globally accessible technologies - - The Notice of Privacy Practices and the registration process should highlight service providers that implement open standards for single sign-on, access delegation via OAuth.,

- Non-coercive - The Notice of Privacy Practices should make it clear that their health records, digitally signed to maintain authenticity, are available for transfer to a PHR or personal server so they do not have to agree to aggregation by the health service provider.

- Standards for information display - The format of the Notice of Privacy Practices should be standardized in the sense that nutrition information labels are standardized.

All of the points above are elements of fair information practice and should be encouraged as part of a respectful patient registration form.

5 - Patient ID Notice

The Notice of Privacy Practices should provide clear indication of what IDs will be used to enable health records aggregation. This notice should be in very plain language and preferably standardized at a national level by some national advocacy group or standards organization. Unlike consent which is subject to state laws and various HIPAA and public health exemptions, patient ID is a constant across all health care services and does not benefit from localization or institutional interpretation.

The Patient ID Notice can be a standard part of the Notice of Privacy Practices.

The Patient ID Notice can be patterned after the familiar W9 form that is used to disclose surveillance of a person's tax liabilities. The fields of the Patient ID Notice might include:

- Name, Address, Sex, DOB
- Voluntary, globally unique Patient ID
- Signature of patient or guardian

If the patient does not have a voluntary, globally unique Patient ID already, the health service provider must create and supply one as part of the registration process. This ID can be created directly by the service provider or using a shared service such as a health information exchange.

If at all possible, the health services provider should provide validation of the voluntary, globally unique Patient ID in order to avoid data entry errors and possible mischief. This is easily achieved if the Patient ID is routable and can cause an email or text message to be sent to the patient as part of the registration process.

Health care service providers should be encouraged to provide a kiosk or equivalent electronic means to fill out and accept the Patient ID Notice. If digital signatures are not available, the Patient ID Form can be printed out for the patient to sign.

In some cases, a health care service provider will have access to a master patient index (MPI) operated by the state or insurance providers. In those cases, the service provider is encouraged to use that master patient index to pre-fill the Patient ID Notice while still allowing the patient to change any of the fields on the form if they choose. The health service provider should not forward any information to the MPI unless explicitly authorized by the patient to do so as disclosed in the Notice of Privacy Practices.

If a patient agrees to forward Patient ID information from the health services provider to an aggregator that operates a MPI (e.g.: a state health information exchange), that MPI is not to be used for health records aggregation. The only permissible use of the MPI is to detect multiple IDs for the same patient and enable the agency, if they choose, to contact the patient and to verify that the patient's use of separate IDs is intentional. If separate IDs were created accidentally, typically because the patient forgot that they already had a voluntary patient ID, then it is up to the patient to merge separate identities by notifying the appropriate service providers.

6 - Patient ID Format

The preferred format for the voluntary, globally unique Patient ID has not been finalized. Patient Privacy Rights proposes this ID be based on a secure Direct email address. Other candidates include regular email addresses, cell phone numbers and globally unique identifiers issued by various public or private institutions.

PPR favors the use of a Direct email address because, when combined with a self-signed certificate, this technology offers both security and privacy with a minimum of reliance on public or private service providers and no proprietary encumberances. Direct email addresses depend only on the functioning of the global DNS or DNSSEC domain routing service that underlies the operation of the Internet.

A patient ID that is linked to a single sign-on capability offers significant usability and security benefits to the patient.

The Patient ID can be linked to a number of other uses to enhance the patient's experience. The outline below lists some of these opportunities:

- Applicability Statement for Secure Health Transport
- PPR Comment to HITPC and HITSC
- Patient ID Issuers
  - HIPAA CE (provider or insurer)
  - State HIE
  - PHR
  - Self
- Optional Patient ID Certifications
  - NICS
  - PDMP
  - APCD
  - Federal Health System (VA / DoD)
  - Medicare (shift away from SSN)
  - Medicaid (reduce churn relative to state health insurance exchange programs)