



The problem

Privacy of healthcare information is complex

The privacy needs of each individual will vary

Many diverse EHR systems are installed today – there is no common approach to managing the privacy of healthcare information

The requirements for a solution

Privacy must be individualized to meet each patient’s unique medical conditions

Patients must be empowered to manage their health information

Any solution must be simple enough for patients to fully understand such that they can meet their privacy requirements

A solution must work with existing systems with little modification required

Restricting dissemination of certain health-related information must be the choice of patients with advice from their physicians

Any solution must not threaten patient safety or quality of care

In certain emergency situations, patients’ privacy wishes may be overridden but must be able to be restored once the emergency is past

A solution must make it difficult to make mistakes but must also provide a mechanism to easily, quickly and inexpensively correct errors

Similarly, a solution must provide a quick, inexpensive recovery from incidents of identity theft or fraudulent use

One solution to consider

Segment healthcare data within the patient record to allow “private” information to be maintained separately from “open” information

Patients voluntarily choose to obtain an “open” identifier to manage the segment of their health record that they wish to make available to all providers across the country



Patients voluntarily choose to obtain one or more “private” identifiers to independently manage those segments of their health record that they wish to be released in a limited manner that they control

Equip patients with tokens that contain their identifier(s) such that they can play an active role in managing their healthcare information

Privacy policies will be independently implemented by various healthcare stakeholder organizations to provide choice for patients and ensure manageability of the solution. In the interim, patients can use private identifiers to manage the privacy of their clinical encounters. Implement a “break-the-glass” option for providers to use in the event of an emergency. After the emergency the patient’s privacy wishes may be re-instated by terminating the patient’s identifiers and issuing replacements

Fraudulent use of a patient’s identity, identity theft and serious errors may also be resolved by terminating identifiers and issuing replacements

Examples

Patients who have no privacy concerns may voluntarily obtain one “open” identifier which is used for all healthcare encounter information

A patient wishes to restrict access to psychiatric encounters. She requests and uses a “private” identifier for all psychiatric visits and uses her “open” identifier for all other visits

For more information

Should you be interested in exploring this topic in more depth, please follow this link for a full copy of the privacy white paper: <http://www.gpii.info/sites/default/files/documents/privacywhitepaper5-21-13.pdf>

Additional information about the Voluntary Universal Healthcare Identifier system can be obtained at www.gpii.info.