WISHIN Pulse Statement on Privacy, Security and HIPAA Compliance

SEC-STM-072014

07/2014

Contents

Patient Choice 2
Security Protections 2
Participation Agreement 2
Controls 3
Break the Glass 3
Auditing 3
Privacy Protections 4
HIPAA Compliance 4
State Law Compliance 5
Special Protection for Sensitive Information under State and Federal Law 5
Limited Access 6

The Wisconsin Statewide Health Information Network (WISHIN) is dedicated to protecting the health information of Wisconsin patients when it moves through WISHIN Pulse, the statewide health information exchange (HIE). WISHIN Pulse is a subscription-only service for health care providers that facilitates the sharing of patient information for treatment purposes. This Privacy, Security, and HIPAA Compliance Statement provides an overview of the privacy and security protections that are part of WISHIN Pulse.

Patient Choice

WISHIN stakeholders agree that health care providers are able to provide the best care when they have access to all of a patient's health information. That said, it is WISHIN's policy, subject to certain exceptions, to provide patients the opportunity to decide whether their health information is shared through WISHIN Pulse. Patients who decide that they do not want their health information shared via WISHIN Pulse can make that choice by completing a Patient Choice Form indicating they wish to "opt out", and submitting the form to WISHIN. Patients who decide they do want their health information shared via WISHIN Pulse do not need to do anything – participation is automatic.

Patients choosing not to have their health information shared through WISHIN Pulse must fill out a Patient Choice Form indicating their desire to "opt out" and send the completed form to WISHIN by regular mail. The Patient Choice Form is available on the WISHIN website, http://www.wishin.org/ForPatients/PatientChoice.aspx, and may also be made available to patients when they register for their appointments with their health care provider. Patients completing the form must clearly indicate on the form the desire to "opt out" of WISHIN Pulse and must provide the specific information requested on the form for the request to be put in place by WISHIN.

The Patient Choice Form includes a list of "opt out stipulations" that describe what will happen if a patient opts out of having their information shared through WISHIN Pulse. This list gives patients important information about the risks associated with their decision to opt out. One of those risks is that opting out may limit the health care information available to their health care providers when they are being treated - and may limit their provider's ability to provide the most effective care. Each patient who submits an opt out request is asked to read and understand that list of stipulations before submitting the request.

Even if a patient chooses to opt out of WISHIN Pulse, a participating provider will still be able to access the patient's health information using WISHIN Pulse for emergency treatment and for public health reporting, such as reporting of communicable diseases or suspected incidents of abuse.

A patient's decision to opt out of WISHIN Pulse will not impact other means of sharing patient information. Even where a patient has filed an opt out choice for WISHIN Pulse, providers and health plans may continue to share patient information through other means (such as by facsimile or e-mail).

A patient who has filed a Patient Choice Form designating their desire to opt out of sharing their patient information with WISHIN Pulse may change that decision at any time by completing a new Patient Choice Form and designating their desire to "Opt Back In". This will revoke their previous opt out designation. This form is available at http://www.wishin.org/ForPatients/PatientChoice.aspx.

Security Protections

Participation Agreement

To participate in WISHIN Pulse, an organization must agree to the terms of the WISHIN Data Sharing Participation Agreement. By entering into this agreement, participating organizations agree to use WISHIN Pulse to access patient information only as allowed by the terms of the agreement. Among other things, the agreement requires participating

organizations to comply with applicable laws regarding the privacy of patient information (e.g., HIPAA) and to implement a number of specific privacy and security protections. Because all participating organizations must execute a participation agreement, any organization that makes its patient information available through WISHIN Pulse has the agreement of other participating providers that any sharing of that patient information will be done in accordance with the terms of the agreement and in compliance with applicable law.

Controls

WISHIN Pulse allows health care providers to control access to the patient information that they maintain. WISHIN Pulse uses a "delegated administration" model and pushes the end-user administration to those closest to the users — the health care providers. System administrators at each participating organization are the only individuals permitted to authorize a user to access WISHIN Pulse. System administrators also assign each user a role that determines the amount of access that the user will have to patient information in the system. Each user is assigned access rights based on their role in their organization (*e.g.*, physician, nurse, administrator, etc.).

For end users, the system uses configurable authentication with password strength checking, attribute-based access controls (ZBAC), and role-based access controls (RBAC). These controls are used to restrict access to information with a high degree of granularity. In addition, automatic account lock-outs and time-outs are employed.

Break the Glass

WISHIN Pulse includes a functionality that allows authorized users to "break the glass" to access patient information in appropriate treatment situations, such as in an emergency. Before "breaking the glass," a provider must certify that he or she has proper authority to access the patient information being requested. Provider access using the "break the glass" functionality is audited, as discussed below.

Auditing

Because WISHIN Pulse tracks each individual user for all significant activities in the system (such as viewing a patient record), authorized Security and Privacy Officers at participating organizations and at WISHIN are able to audit individual user activity. Privacy and Security Officers are able to generate audit reports that detail the various ways in which their users have accessed WISHIN Pulse. For example, a hospital is able to see the number of times any of its users queried a patient or the number of times a certain user "broke the glass." Users are subject to sanctions for any inappropriate access.

One of the main goals of WISHIN Pulse is to improve upon the status quo with respect to the sharing of health information between providers for treatment purposes. To that end, WISHIN and its participating organizations agree that WISHIN Pulse is more capable of protecting the privacy of health information than many of the current systems used by medical practices, many of which still rely on paper records. For instance, in current systems, when one provider wants to share a patient's clinical information with another provider, that information is typically faxed to the second provider's office. Any number of office staff have access to that fax and there may be no record of who actually receives it, views it, or files it. With WISHIN Pulse, by contrast, clinical information can be viewed only by designated individuals. Participating organizations agree to designate authorized users in accordance with applicable law and the terms of the participation agreement so that access to patient information is restricted to those individuals who have appropriate authority to view it. Further, WISHIN Pulse has the ability to track each person who accesses patient

information. In this way, WISHIN Pulse offers far greater auditable privacy protections than many of the current systems for sharing health information.

The computer systems and servers that make up WISHIN Pulse can be managed either by the participating organization or, if desired, they can be hosted and managed on behalf of the participant and WISHIN by a hosting service such as Medicity (which is a hosting vendor with which WISHIN contracts). Regardless of where the systems are hosted or who manages them, the data remains the property of the participating provider. When hosted and managed by Medicity, the systems are housed in redundant, Tier 4, SAS 70 Level II compliant data centers protected by a variety of perimeter defense systems including firewalls, intrusion detection systems, intrusion prevention systems, and a 24x7x365 Network Operations Center. A participating organization may access WISHIN Pulse only via strongly encrypted communication channels.

WISHIN Pulse protects data while in motion and while at rest via multiple mechanisms such as SSL, PKI, one-way hashing of certain data types such as user passwords, and symmetric encryption of clinical data at rest. The following encryption is used to protect data:

- 128-bit TLS or SSL encryption. SSL encryption is used for all browser display and data transmitted via web services.
- HIE Transmission Security. Connections between WISHIN Pulse and participating organizations are completed across a VPN (**V**irtual **P**rivate **N**etwork) tunnel and are limited via access control lists (ACLs) to specific hosts within the organizations. In addition to encrypted channels, a network of trust is established, driven off of a private key infrastructure (PKI). Intrusion Detection Software (IDS) is used to detect any malicious traffic across the networks.

Privacy Protections

HIPAA Compliance

The federal Health Information Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules protect the privacy and security of certain types of patient information known as “protected health information” or “PHI.” Most of the patient information that is transmitted using WISHIN Pulse would be considered PHI. Both WISHIN and the providers who use WISHIN Pulse are subject to HIPAA’s Privacy and Security Rules. (WISHIN is a HIPAA “business associate,” and participating providers are generally HIPAA “covered entities.”)

The HIPAA Privacy Rule restricts the manner in which PHI may be used or disclosed. In general, a covered entity or business associate may not use or disclose PHI except as permitted by the Privacy Rule. Certain types of uses and disclosures require patient authorization, while others do not. For example, no patient authorization is required for the disclosure of PHI to a health care provider for purposes of treatment. This is the primary type of disclosure that is made using WISHIN Pulse and it is specifically authorized by the Privacy Rule.

In addition to the Privacy Rule’s restrictions on the manner in which PHI may be used and disclosed, both the Privacy and Security Rules impose certain requirements in regard to protecting the privacy and security of PHI. WISHIN has taken measures to comply with these requirements

State Law Compliance

Similar to HIPAA, Wisconsin law (Wis. Stat. § 146.82) requires that all patient health care records remain confidential and, generally, records may be released only with the patient's informed consent. However, also similar to HIPAA, Wisconsin law recognizes that health care records generally may be disclosed without the patient's informed consent to a health care provider who is providing treatment to the patient; to the extent the records are needed for billing, collection or payment of claims; and for purposes of health care operations, as defined and authorized under HIPAA, as well as for certain public health activities and other specific lawful purposes. WISHIN Pulse is primarily used to share information for treatment purposes, which is permitted under §146.82.

Special Protection for Sensitive Information under State and Federal Law

Both federal and state laws extend special protection to certain types of health information that WISHIN refers to as "sensitive data" or "sensitive health information." In some cases, these state and federal laws impose different or more stringent requirements regarding the sharing of patient information than the requirements imposed by HIPAA. Click here for examples of such federal and state laws.

Each organization participating in WISHIN Pulse is responsible for complying with applicable laws and its own policies with regard to identifying and providing special treatment for information subject to special protection. Participants will refer to federal, state and local laws for full restrictions on sharing and accessing information subject to special protection.

WISHIN facilitates compliance with the state and federal laws that provide special protection to sensitive data as follows:

Sensitive Data Will Be Disclosed Only in a Medical Emergency

"Sensitive data" or "sensitive health information" will be accessible through WISHIN Pulse only when the health care provider treating the patient has certified that the patient has a medical emergency and is not able to give consent.

Prominent Identification of Sensitive Data

Health care organizations that share sensitive data through WISHIN Pulse must identify the health data as being "sensitive" in accordance with WISHIN's policies and procedures. Health information flagged as "sensitive" will only be available through WISHIN Pulse in an emergency when the patient is unable to give consent.

Notation of Disclosure in Patient's Records

WISHIN maintains an audit log for each participating organization that includes the name of the person to whom the sensitive data was released and their affiliation to any health care facility, and the date of the release.

Some information subject to special protection under state and federal laws must not be shared through WISHIN Pulse. Participants are responsible for identifying this information and ensuring that it is not sent through WISHIN Pulse. Examples of information that Participants must not share through WISHIN Pulse:

No Psychotherapy Notes, AODA Records Maintained in Connection with a Federally Assisted AODA Program, or Records of HIV Results from a Compelled Test

Participants must not use WISHIN Pulse to share (1) "psychotherapy notes," as defined in HIPAA, 45 CFR §164.501, or (2) HIV test results from a test that was compelled under Section 252.15(5g) of the Wisconsin Statutes as a result of "significant exposure", or (3) records subject to 42 CFR Part 2 (*i.e.*, AODA treatment records maintained in connection with a federally-assisted AODA program).

Limited Access

In respect of each patient's privacy, WISHIN will limit access to a patient's protected health information to only those health care providers who have an established treatment relationship with the patient. Each participating organization has valid and enforceable agreements with each of its participant users requiring the participant users to:

- Comply with all applicable laws, including HIPAA, HITECH, and Wisconsin statutes;
- Use WISHIN Pulse only for permitted purposes, specifically for the treatment of a patient;
- Report a potential breach to appropriate personnel as soon as reasonably practicable; and
- Refrain from disclosing any passwords/PIN numbers or other security measures issued to the participant user.