Health Information Technology and Health Information Exchange: Privacy Principles for Protecting Victims of Domestic Violence

September 2013

Health information technology (HIT) has the potential to help providers screen for domestic and intimate partner violence (DV/IPV), and to guide them to appropriate services and ways to coordinate care. That said, there are privacy concerns unique to women who have experienced domestic violence. Who has access to electronic medical records and health data? What are the consequences of any breach of confidentiality to medical records by health care staff? For victims of DV/IPV, this is not just an issue of privacy but also one of safety as perpetrators of DV/IPV can retaliate against victims of abuse if they find their partner has discussed violence with their provider.

Technology can be used to prompt providers in different health care settings to screen for domestic violence and to provide the appropriate "best practices" for responding. It can also improve care coordination, and be used to promote quality improvement as it relates to response to DV/IPV. When domestic violence is detected, an electronic health record can prompt providers to the correct referrals, counseling and services to make sure that women get the help they need. Furthermore, given the long-standing health effects of domestic violence, including an increased likelihood of chronic conditions such as diabetes or asthma, HIT is invaluable in coordinating between providers and providing seamless coverage to manage these long-term health effects.

Clinicians and administrators must create an environment that prioritizes the safety of victims including respecting the confidentiality, integrity and authority of each victim over their own life choices. Federal legislation and state and local statutes are crucial to establishing a comprehensive baseline of regulations and protections for the use and disclosure of sensitive electronic information. HIT developers and vendors also have a role in building the software and hardware necessary to deal with the information in an appropriate fashion.

Below are guiding principles that should be applied by clinicians, administrators, policy makers and developers when designing, building or regulating health information systems that will hold or exchange sensitive health information. These principles build on past work to protect information collected in paper health records, and expand the consideration to electronic health records and health information exchanges.

Principles

Policy and practice surrounding the use and disclosure of health information—on paper or electronic—should respect patient autonomy and confidentiality while trying to improve

the safety and health status of a patient. There should be strong and enforceable penalties for failure to comply with privacy rules and regulations.

- Personal and sensitive health information should be de-identified whenever possible;
- Individuals should have the right to access, correct, amend, and supplement their own health information;
- Individuals should receive notice of how health information is used and disclosed, including specific notification of the limits of confidentiality;
- Providers must offer and respect patient's choice of communication preferences, including by phone, by email, etc, and under what circumstances. This should be built in to electronic health records as mandatory fields;
- Privacy safeguards and consents should follow the data;
- Providers should have broad discretion to withhold information when disclosure could harm the patient;
- There should be strong and enforceable penalties for violations of privacy and consents both in a clinical setting, and across information exchanges.

De-identified Information
Personal and sensitive health information should be de-identified whenever possible

Health data shared across clinical settings or in data collection should be de-identified; it should not identify individual patients. Information that could identify a patient—such as name, social security number, or address—should be removed or redacted wherever possible. This protection extends to government or private data collection.

Health information technology helps make it easier to de-indentify data by building systems to establish de-indentified data collection. It is important that federal and state guidelines be in place to ensure that the technology is put in place and that appropriate use of de-identifies is maintained across all data exchanges.

In cases where identifiable patient data may be shared or exchanged, patients should give written authorization to share these data. Patients should have the right to restrict the use or disclosure of identifiable data beyond certain core functions (such as treatment and payment between a provider and a health plan).

Patient Access and Notice
Individuals should receive notice of how health information is used and disclosed, including specific notification of the limits of confidentiality

Individuals must receive notice of how their health information is used and the circumstances under which it could be disclosed. With full information, victim can better evaluate if and how to share their data, and under what circumstances they choose to

disclose. There are specific federal HIPPA guidelines that establish federal notification rules about privacy and disclosure of health information[i]. They establish how patients are to be notified of their rights, how patient data could be used, and how the provider or plan safeguards their data.

In states where there are mandatory reporting requirements, providers have a responsibility to share those reporting requirements. When information is going to be released by a provider (such as in the case of mandatory reporting) a victim should be notified of the disclosure. Victims can then choose not to voluntarily disclose and/or can work with their provider to figure out how to move forward. It is vital that a victim feel that the confidentiality requirements will provide adequate protection.

A woman was injured by her partner and went to the hospital. She was afraid to go inside because she was unclear about her state's mandatory reporting law. She spent the night in her car in the hospital parking lot and did not receive necessary medical treatment for the injuries she sustained.

Individuals should have the right to access, correct, amend, and supplement their own health information

Individuals have a right to access and request a copy of their health record—on paper or, now, electronically[ii]. And they have the right to modify that record. In the cases of a victim of DV/IPV, the ability to review records—particularly in an electronic format—may increase trust in a provider and a deeper understanding of how her confidentiality is being protected. If she can see that information is done in a certain way, she may be more willing to trust that provider and not assume that inaccurate or incomplete information can result in retaliatory violence if viewed by the abuser, or embarrassment. It would also give her the ability to change her privacy settings, contact information, or consents from a safe, remote location if necessary.

Patient Communication

Individuals should be given choices of how they would like to communicate with—and receive communications from—their providers and plan, including by phone, by email, etc, and under what circumstances. This should be built in to electronic health records as mandatory fields.

There are real privacy concerns for women who have experience DV/IPV, and policymakers must recognize the unique communication preferences these women may have. Abusers could be monitoring email, phone numbers or benefits statements. Or a

woman who is covered by the employer-based coverage of her husband may have her billing statements and Explanations of Benefit statements will go to him as the policyholder. It is vital that providers recognize that and carefully document communication preferences. Providers are in a trusted position to provide support and services but it must be done in such as way as to respect the needs of the individual patient.

We underscore the necessity for reminders being sent ***per patient preference.*** It is critical that providers do communicate with patients per the patient preference, as there are real safety and privacy concerns to be considered for women who are in an abusive situation. All patients who disclose abuse should be offered preference on how or if follow up communication should take place, and no specific mention of DV verbally or in writing should be made in the follow up reminders. It is also vital that payors, such as insurance companies, develop and adhere to best practices for not printing certain sensitive codes on these types of documents.

Victims should be permitted to provide alterative contact information for different types of communications as well. If a woman's receives her insurance coverage through her husband's employer, his address and email may be primary on the account. She should never be required to have communications go to someone other than who she chooses.

A woman came to Massachusetts after escaping a physically and emotionally abusive relationship. The abusive partner told her that she could remain on his insurance plan until she found her own, but, since he does not know that she is in Boston, she fears that he will use insurance notices as a way to keep tabs on her whereabouts. She did not see another provider for over a year, until she was forced to seek care for a pregnancy test. While she has decided to continue the pregnancy, she is struggling to find other options for insurance and remains very worried that her former partner will both find out where she is and find out about the pregnancy through the EOB.

Considerations for Information Exchange

When health data are exchanged between providers, plans, and other entities, a patient must give consent for the data to be shared ("pushed") or retrieved ("pulled") by other entities.

Health Information Technology provides opportunities for detailed care coordination across multiple care settings. Exchanging health information between providers and having information following the patient has the ability to help lower cots and provide a holistic approach to treating the whole patient. While safety concerns should be paramount, a

noted history of DV/IPV can lead to improved care coordination for patients over the course of the lifespan. Women who have experienced DV/IPV were more likely to experience long-term chronic diseases, such as asthma and diabetes. They reported frequent headaches, chronic pain, and overall poor mental and physical health[iii]. A full

history may help providers monitor and treat for these conditions and improve long-term health outcomes for victims.

There are new and emerging safety and privacy concerns with the move to electronic health information exchange, and with the ability of the whole care team to access a patient record. The policy governing these types of exchange are being developed now and safety questions must be addressed. How will sensitive health information be redacted or blocked so that only providers that the victim gives permission to has access to the data?

In building formal health information exchanges, there must be standards developed that dictate the circumstances under which a provider—or anyone with access to the medical records—is allowed to access them. For example, can a hospital worker access their colleagues' records without explicit permission? There needs to be a reason and set of permissions before an individuals record is available to be "pulled" through an exchange.

It may take a long time for a victim to find a trusted provider to whom to disclosure the abuse. It is to this one provider that she is disclosing, not to her whole team of providers. She may have concerns about her other providers knowing. If she discloses to her GP, can her podiatrist also have access to those records? Can the podiatrist "pull" those data through a trusted health exchange? What if the podiatrist if the abuser or related to the abuser?

Privacy and consents should follow the data

All privacy and signed consents should follow the data, regardless of who is using it. If a provider "pulls" data on a patient, the data receive should be automatically subject to the same consents that a patient signed in the originating encounter. Responsibility for adhering to these consents must be built in to the formal health information exchange trust documents—and there must be strong penalties for breaching these privacy concerns.

Certain data or diagnosis codes should be always redacted from push/pull functionalities. Where sensitive conditions cannot be blocked, patients must be informed and give written consent to share those data in health information exchanges.

Providers should have broad discretion to withhold information when disclosure could harm the patient.

Patients and providers must be given the opportunity to "break the glass" and to implement a system safeguard that would block all health data from exchange and/or

viewing. In sensitive cases, in high profile cases, or where there is an immediate and real safety concern, the patient or their provide should be able to prohibit viewing of the electronic health record—or parts of it—from all outside sources.

A woman discloses current abuse to her GP—but shares that the abuser is a provider in the same health system who has access to all patients EHRs, including hers. The provider enables protections on the patient's personal information so that all external viewing of the patient's data are prohibited.

A prominent local celebrity discloses abuse. Her provider "breaks the glass" to prohibit any hospital employees from viewing the information without patient permission.

There should be strong and enforceable penalties for violations of privacy and consent both in a clinical setting, and across information exchanges.
Whether due to negligence or oversight, violations of privacy and consents should be penalized to the fullest extent of the law. The penalties should be strong enough to deter future cases, and they must be enforceable.

---

[i] http://www.hhs.gov/ocr/privacy/index.html
[ii]http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/righttoaccessmemo.pdf
[iii] National Intimate Partner and Sexual Violence Survey; CDC, December 2011.

The National Health Resource Center on Domestic Violence (HRC) is the nation's clearinghouse for information on the health care response to domestic violence and provides free technical assistance and materials. The HRC is funded by a grant from the Family Violence Prevention & Services Program, Family & Youth Services Bureau, Administration for Children and Families, U.S. Department of Health and Human Services. For more information, please visit www.futureswithoutviolence.org/health or contact health@futureswithoutviolence.org or 415-678-5500.