HEALTH PARTNERS ON IPV + EXPLOITATION

Privacy Principles for Protecting Survivors of Intimate Partner Violence, Exploitation and Human Trafficking in Healthcare Settings

Health information technology (HIT) is a crucial tool for healthcare systems to coordinate care for patients, yet there are privacy concerns unique to people who have experienced intimate partner violence (IPV) and exploitation. With potential impact to a patient's care utilization and engagement, this is not just an issue of privacy but also one of safety. While these concerns are relevant to other sensitive and stigmatized health information, IPV/exploitation survivors, specifically, may consider:

- What is written in my electronic medical record about my experiences of violence and other sensitive health information?
- Who has access to my electronic medical record and health data?
- What will happen if my partner finds out that I have been talking to my provider about the violence?
- How will I be treated differently if other people on my care team know that I am surviving violence?
- Will my health insurance or payer send an explanation of benefits to my address?
- What control do I have over my health information and what are my rights as a patient and as a survivor?

The landscape of HIT is rapidly evolving, as is data collection on IPV in health settings. In 2020, the Health Resources and Services Administration introduced new Uniform Data System (UDS) measures that require all federally qualified health centers to collect data on disclosures of IPV and HT.[1] It is vital that healthcare providers consider the ways that electronic medical records and data sharing could decrease safety for IPV survivors and take steps to ensure that patients who are surviving abusive relationships are in control of their own health information. These steps become even more critical as identification and documentation of IPV increases, patients receive expanded access to their own health information, and coordinated care is broadened to include services that address social determinants of health. Health systems and providers should review these principles and establish a working group including representatives from all specialties and including Health Center Controlled Networks (HCCNs) when appropriate to implement changes.

[1] https://bphc.hrsa.gov/sites/default/files/bphc/datareporting/pdf/2021-uds-manual.pdf

Below are guiding principles that should be applied by healthcare providers, administrators, policy makers and developers when designing, building, utilizing or regulating health information systems that will hold or exchange sensitive health information.

Privacy Principles

For patients who are experiencing abuse and control from a partner, family member, or employer, this is not just an issue of privacy but also one of safety. Policy and practice surrounding the use and disclosure of health information should respect patient autonomy and confidentiality while trying to improve the safety and health status of a patient.

- Patients should receive an explanation of how health information is used, shared disclosed, including specific notification of the limits of confidentiality;
- Patients should be made aware of their rights to access, correct, amend, and supplement their own health information;
- Personal and sensitive health information should be de-identified whenever possible;
- Providers must offer and respect patients' choice of communication preferences;
- Privacy safeguards and consents should follow the data and the limitations on consents should be clearly identified if/when health data is shared with another provider who may not have the same privacy settings;
- Providers should have broad discretion to withhold information when disclosure could harm the patient as per provider determination and on an ad hoc basis;
- Systems should be set up to allow for sensitive information to be partitioned between providers when appropriate;
- There should be strong and enforceable penalties for violations of privacy and consents both in a clinical setting, and across information exchanges.

Privacy principles relate both to documentation as well as clinical encounters. In addition to setting up systems to keep medical records as private as possible, some portion of the visit should always be conducted in private when discussing IPV/HT.

Explanation of health information, data sharing, and confidentiality

Individuals must receive notice of how their health information is collected, used, and the circumstances under which it could be shared. When documenting experiences of IPV, other forms of violence, and other sensitive health information in the medical record, it is crucial that providers discuss with patients:

- what is being documented
- how it is being documented
- why it is being documented
- circumstances under which the information could be shared
- and who may have access to this information, including potential scenarios where information could be accessed without authorization.

"You mentioned that your partner sometimes keeps you from taking your insulin. Would it be okay if I note this in your medical record? It might be useful for others on your care team to know when you see them so that they can provide the best care for you. I would notate it discreetly in an area of your medical record that does not show up on your patient portal or explanation of benefits."

With this information, patients can better evaluate if and how they would like their data documented and shared. There are specific federal HIPAA guidelines that establish federal notification rules about privacy and disclosure of health information. 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. However, because the notice of HIPAA guidelines is often provided quickly in writing and without meaningful explanation, specifically discussing documentation is important. In the few states where there are still mandatory reporting requirements for injuries caused by IPV, and ***providers have a responsibility to share those reporting requirements before engaging in conversations about how relationships affect health***. With this information, patients can choose not to voluntarily disclose and/or can work with their provider to figure out how to move forward. It is vital that survivors feel that the confidentiality requirements will provide adequate protection. When information is going to be released by a provider (such as in the case of mandatory reporting) a victim should be notified and be invited to participate in the mandatory reporting process to the extent that they want to.

If a patient decides that it is not safe to include any kind of documentation about IPV in the medical record, it can be useful for that providers to explain how this may limit the ability of others on the care team to provide trauma-specific care. Providers can indicate:

"We can definitely leave this out of your medical record, and I want to give you a heads up that others on your care team will not have this background information when you see them next."

21ST CENTURY CURES ACT

In an effort to increase patient empowerment, the 21st Century Cures Act works to create transparency about patients' health information and costs. New federal rules on the sharing of healthcare information/data went into effect in April 2021. These rules were put in place to stop the practice of "information blocking" and to promote better coordination of care. The rules require that provider requests for electronic health information, including most clinical notes, should be acted on and the information requested be shared between providers. These rules specify that the sharing of clinical notes must not be blocked from information exchanges unless an exception applies or there is a good reason why the information will not be shared. There are specific exceptions if sharing the information could cause harm to the patient and health providers and systems should consider any conversation about IPV/Exploitation including universal education, screening or referrals as sensitive and that therefore should not automatically be shared unless the patient requests it. Additionally, care must be taken when considering what information appears in the patient portal. As of April 5, 2021 clinical notes must be shared with a patient by the health systems by April 5, 2022 if requested and shared with a patient's 3rd party apps by October 6, 2022. However, this information should not be automatically populated without a patient's consent and request. Learn more at futureswithoutviolence.org.

Patients' rights to access, correct, amend, and supplement health information

All individuals have a right to view and modify their medical record. With the passage of the 21st Century CURES Act, this access has increased so that patients can view all notes in their medical record if requested. Patients should be made aware of how they can access, correct, and supplement their health information. Information should not be auto populated into clinical notes or patient portals without patient consent and request and until policies are in place to safeguard sensitive information. Particularly for survivors of IPV, knowledge of how to do this could increase safety from abuse and promote trust in their provider and care team. This conversation also provides the opportunity for patients to change their patient portal privacy settings, contact information, or consents.

HEALTH RECORD DOCUMENTATION

It is important to keep any descriptive documentation to minimal phrasing, unless otherwise indicated by the patient. Example documentation:

Documenting universal education about how relationships impact health and available resources offered:

"Universal education offered"

Documentation with disclosure of intimate partner violence:

"Universal education offered, health promotion and harm reduction strategies shared, referrals offered, and follow up discussed."

Learn more about universal education for IPV/exploitation.

De-identified information

Personal and sensitive health information should be de-identified whenever possible; 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 makes it easier to de-identify data by building systems to establish de-identified 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-identified data is maintained across all data exchanges.

CODING FOR VIOLENCE AND ABUSE

Providers are increasingly coding for assessment and disclosures of abuse, human trafficking, and other forms of violence. IPV and HT were added to the UDS report in 2020 and community health centers must now collect UDS data on disclosures of IPV or disclosures or concern for HT/exploitation. Coding for violence and for offering brief counseling can allow health systems to collect data on the number of patients who feel safe disclosing violence and potentially may enable reimbursement for providing brief counseling to survivors. Ensure that codes that indicate any form of violence and abuse are not included on the Explanation of Benefits (EOB). For more information about coding and specific ICD10 and CPT codes that are relevant to use visit futureswithoutviolence.org.

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), however billing processes will require an exchange of personally identifiable information. Explanation of benefits inherently contain personally identifiable information, but can be made safer through better coding and changes to EOB policy.

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, as there are real safety and privacy concerns to be considered for patients who are in an abusive situation. Abusive partners could be monitoring email, phone numbers, or benefits statements. Providers are in a trusted position to provide support and services but it must be done in such a way as to respect the needs of the individual patient.

Preference on how or if follow up communication should take place should be built into the health record as a mandatory field. For patients who have disclosed abuse, no specific mention of IPV verbally or in writing should be made. 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.

EXPLANATION OF BENEFITS

Explanation of Benefit (EOB) documents are letters generated by a health insurance company that describe what benefits have been covered for their members. EOBs can make health insurance more transparent by explaining the benefit coverage and limits for the policy holders, minimizing billing surprises, and reducing fraud or waste.

These documents contain potentially sensitive information—such as the name of provider practice (e.g., a mental health counselor or a reproductive health clinic) and description of services provided, and there are many considerations about how this information could impact survivors. This is especially because EOBs are sent to policy holders, not necessarily to the patient themselves. This could impact patients who are not the policyholder, including victims of IPV/HT; young adults to age 26 who get their health insurance through their parents' plan; and minors who want to access health services without their parents knowing and/or without parental consent.

It is important that providers educate patients about the limits of confidentiality, what EOBs are and how information could be shared with the primary policy holder. For example, some adolescent patients may have concerns about parents or guardians being the policy holder and receiving information about sensitive services. Adults also may be concerned about information sent home so other family members can see it. More information about opportunities to strengthen and improve the confidentiality of EOBs can be found at futureswithoutviolence.org

Privacy and consents should follow the data

All privacy and signed consents should follow the data, regardless of who is using it. If a survivor's health information is shared with another provider, the data received 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 into the formal health information exchange.

CARE COORDINATION PLATFORMS

Increasingly, healthcare providers are utilizing online tools as part of their practice. These may include supported referral and coordination networks or other online resources to connect their patients with the social supports and non-medical services they need. For example, a provider may use a hyper-local referral network that can allow them to give a targeted list of community resources to their patients. While a warm referral and solid partnership between a provider and a domestic violence service provider is the most effective solution, these types of tools can provide real-time direction to survivors.

There are many different models for these types of networks and some networks provide an excellent service with deep community expertise. Local domestic violence service providers or state domestic violence coalitions can help providers better understand which services and tools are trusted in the community.

Because these tools collect sensitive health information and track patient data, it is extremely important to safeguard sensitive information and to be very careful with what information is shared with the online platform. All of the privacy principles listed in this document must adhere to the sharing of health information with these online tools.

Provider discretion

Providers should have broad discretion to withhold information from data exchange when disclosure could harm the patient. Patients and providers must be given the opportunity 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 provider should be able to prohibit viewing of the electronic health record—or parts of it—from all outside sources.

Sensitive information partitioning

Electronic medical record platforms should be changed or developed to allow for the ability of providers to make closed or private notes that may impact care provision, but are only visible to designated members of the care team who are granted permission and not visible to the entire health system. This information should not be shared with other providers without explicitly permission from the provider or patient, and should never be automatically uploaded into a patient portal.

Violation enforcement

There should be strong and enforceable financial 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 incur penalties strong enough to deter future cases.

CONCLUSION

Providers and administrators must create an environment that prioritizes the safety of victims including respecting the confidentiality, integrity and authority of each survivor 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.

Given the long-standing health effects of IPV, including an increased likelihood of chronic conditions such as diabetes or asthma, it is critical that providers discuss IPV/HT and its impact on health. HIT is invaluable in coordinating between providers and providing seamless coverage to manage these long-term health effects. It is critical however that a plan is put into place to conduct those conversations safely and keep information confidential. The electronic health record can prompt providers to the correct referrals, counseling and services to make sure that patients get the help they may need for themselves or others in their families or communities.

KEY RESOURCES

Guidelines Documenting ICD-10 Codes and Other Sensitive Information in Electronic Health Record

Explanations of Benefits & Safeguarding Sensitive Health Information

Learn more at futureswithoutviolence.org.

ACKNOWLEDGEMENTS

This publication is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of awards as follows: U30CS39198 totaling $725,000 and the FVSPSA National Health Resource Center on Domestic Violence with 0 percent financed with non-governmental sources . The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit HRSA.gov.