FUTURES WITHOUT VIOLENCE

First Steps to Building a Safe EHR for Women

As Electronic Health Records (EHR) continue to develop, there is an opportunity to think through, develop and implement a tool within an EHR for universal assessment and response for domestic and intimate partner violence. There are many vital considerations for privacy and security—and detailed ideas about how best to integrate screening and referral tools. We understand that these will take time fully integrate and we look forward to working with policy makers to implement them.

That said, there are many policies that can be implemented in existing EHRs ***today*** that will have a dramatic impact on the health care and care coordination of women who have experienced DV/IPV.

As policymakers consider Stage 3 Meaningful Use, the discrete actionable items listed below should be adopted in order to make today's technology safe and productive for all patients, and especially victims of DV/IPV.

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. Communication preferences 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.

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[i]. 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.

Exchange of sensitive data

Data for women experiencing DV/IPV should be treated in a manner similar to other sensitive conditions, such as HIV/AIDS or substance abuse. 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.

EHRs should include key elements that prompt providers to screen for DV/IPV—and help providers make appropriate referrals.

EHRs and clinical decision supports systems are tools to help providers screen for DV/IPV, and they work in conjunction with other evidenced-based and recommended interventions, such as the brochure-based universal screening as recommended by the USPSTF.

EHRs should have the capability to prompt providers to screen in a variety of settings.

- **Prompt for DV/IPV in any appropriate setting, providers should be prompted to screen for DV/IPV for every patient.** The questions need to be hard to skip—for example, an answer needs to be provided before a provider can move to the next screen. This is called a "hard stop" and is a powerful tool for encouraging screening questions.
- **Disclose the Limits of Confidentiality.** EHR must include instructions for providers to share with the patient the state-specific limits of confidentiality. The text of this disclosure should be included before the assessment question.
- **Provide Universal Education and Assessment Prompts.** The EHR should provide sample scripts for the provider to offer universal DV education and assessment. To promote universal patient education, the EHR should prompt providers to share a brochure with every patient to avoid a "check box" approach to screening.
- **If DV/IPV is Disclosed, Prompt for Referrals.** To support a strong relationship with local DV advocates in their community, an EHR should also include an regularly updated local DV/SA resource list as well as phone number for the national DV hotline, teen helpline or other national sexual assault resource.

---

[i] http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/righttoaccessmemo.pdf