21st Century CURES Act: A Summary and Recommendations to Promote Patient Privacy for Survivors

April 2024

Futures Without Violence has long supported strong privacy and confidentiality protections regarding the exchange of personally identifiable health information and recommend:

- Robust, informed patient consent about sharing of healthcare data;
- Patient control over how health data is shared and with whom;
- Transparency over who has access to health data and when;
- Sensitive information de-identified whenever possible; and
- Awareness of how and when information shared on plan/billing documents that are shared with the policy holder.

Patients mut be informed about what is being documented; how it is being documented and why; the circumstances under which it could be shared; and who else could access the information. (For more information, read our Privacy Principles for Protecting Survivors of Intimate Partner Violence, Exploitation and Human Trafficking in Healthcare Settings.)

Federal rules on the sharing of health care information and data went into effect in April 2021. Stemming from the 21st Century CURES Act, these rules were put in place to support patient care by promoting better coordination of care and by stop the practice of "information blocking" in which providers are unable to access patient records.

However, for survivors of domestic and intimate partner violence—and the providers who serve them—these new rules raise serious concerns about how survivors' health data will be shared, under what circumstances, and who can have access to the sensitive health information.

The new federal rules **do** contain exemptions for preventing harm and for maintaining privacy that will help support survivor privacy and confidentiality. But providers need a clear understanding of what the new rules mean and what the best practices are for serving survivors—and will need to act to put policies in place.

Though there are many benefits that come from sharing data between providers there are also risks present with the use of any data sharing platform. Survivors and their providers must carefully balance these competing issues.

The new rules support information exchange.
The rules require that requests for electronic health information (EHI), **including most clinical notes**, should be acted on and the information requested be shared. In other words, the rule

creates a presumption that EHI should be shared *when requested*. However, this does not mean that EHI must be disclosed to all requesters, for any purpose. There are number of important exceptions to this rule.

There is no requirement to proactively share or publish EHI *unless requested*.
There is no requirement to proactively make EHI available or to put it in the portal. This rule applies to situations where a provider or a patient *requests* that the information be shared.

Most EHI, including clinical notes, will be subject to this rule.
This rule creates a presumption that EHI should be disclosed, including:

- Consultation notes
- Discharge summary notes
- History and physical
- Imaging narratives
- Procedure Notes
- Progress Notes

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. Psychotherapy notes are separated from the rest of the individual's medical record and are protected by other privacy rules. But they *are* required to share counseling session start and stop times, modalities and frequencies of treatment, and any summary of diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date if the information is request and if the law permits such sharing and there is no other exception that applies.

Other privacy rules still apply.
The CURES Act does not override other health information privacy rules including those set forth in the Health Insurance Portability and Accountability Act - HIPAA). Access is not made any wider than what HIPAA already allows.

There are exceptions to the rules that help protect survivors.
Health providers have broad discretion to withhold data when disclosure could cause harm or because a patient requests it. The rule has eight categories of exemptions, known as safe harbors, under which a provider may decline to share requested data including:

- *Preventing harm*: The provider must believe that the denial will substantially reduce the risk of harm. For record keeping purposes, the process by which providers can apply this exemption should be in writing and applied in a consistent and nondiscriminatory manner.
- *Privacy*: The provider can deny to a data request if an individual's request that the provider not share information or if the provider was unable to obtain patient consent.

Health care providers should have documented policies for applying exceptions.
Each situation is evaluated on a case-by-case basis and in accordance to both the law and the practices documented policies. Every health care practice should have clear and transparent

policies for how they will apply the preventing harm and privacy exceptions to protect survivor confidentiality and autonomy.

The default should be not to post sensitive data unless request.
And all health practices should implement a system safeguard that protects sensitive EHI. As there is no requirement to automatically populate or publish data in a patient's portal, a best practice should be to only publish information when requested and only with patient consent.

Key Resources

- Preventing Harm FAQs
- Preventing Harm (and Exceptions) Fact Sheet
- Exemption webinar slides
- 21st Century Cures Act: Considerations for working with survivors of intimate partner violence
- Information Blocking Exceptions