Texas Council
of Community Centers

Texas Council Privacy and Consent Strategy

The Data Work Group (DWG) of the Texas Council of Community Centers, a project of the Health Opportunities Workgroup (HOW), has been meeting since early 2013 to support the health IT readiness needs of Texas Council Members. One of the major challenges that behavioral health agencies face in participating robustly in a health IT environment is how do to so while maintaining compliance with §42 CFR part 2, the federal substance abuse treatment privacy regulations.

By and large, §42CFR regulations are only incumbent on federally funded substance abuse treatment services—such as those through Medicare and Medicaid—but there is some disagreement about which agencies meet this definition. As a first step, it would be worthwhile to revisit whether and to what extent Texas Council members must abide by these regulations.

Most, if not all, Texas Council members operate as if they are obligated to meet these regulations. Regarding their engagement with HIEs, the main challenge comes in operationalizing them both for providers of multiple services and for HIEs who want to accept content. For providers, there is no easy way to segment substance abuse treatment data that would allow it to be treated differently than data related to other services. As a result, providers have generally adopted an approach of adhering to the most restrictive standard for all their data, not just substance abuse treatment data.

For HIEs, on the other hand, the major challenge comes in the form of operationalizing the "named provider" component of the consent requirement. The Health Insurance Portability and Accountability Act (HIPAA) and subsequent updates is the general framework for requiring informed consent from consumers when health-related data is shared—regardless of with whom. As a result, HIEs must obtain consent from consumers in order to accept and distribute individually identifiable health information such as a consumer's clinical data. Typically, HIEs use consent language that permits an HIE to obtain data and share it with all providers who "participate in the HIE."

If the providers participating in an HIE was perfectly stable, this provision might be sufficient for §42CFR purposes. However, the reality is that HIEs experience significant churn among participating providers. As a result, a patient consent to participate would only be relative to providers in the HIE *on the date the consent was signed.* In order to operationalize this in a manner consistent with §42 CFR, an HIE would have to maintain a list of which providers were participating on which day, and prevent the flow of patient data to providers who were not participating on the day the consent was signed.

Functionally, most HIEs have adopted an approach of being "all or nothing"—meaning they either accept and distribute all data, or the accept and distribute no data. The net result of this, and the high standard adhered to by Council members, is that almost no HIE can accept behavioral health data.

Nonetheless, there is a strong clinical case for getting HIEs to accept behavioral health data. Nearly 70% of individuals with a behavioral health condition have a chronic medical condition, and nearly 30% of individuals with a chronic medical condition have a co-morbid behavioral health condition. Additionally, individuals with behavioral health conditions and chronic medical conditions have costs that are more than the sum of their individual conditions.

The Data Work Group began exploring privacy and consent by reviewing efforts underway elsewhere around the country. In addition to studying materials from HIEs including the Rhode Island Quality Institute, and Maine's HealthInfoNet, the workgroup also reviewed content from different federal agencies. For example, the Substance Abuse and Mental Health Services Administration (SAMHSA) presented on a consent management tool they are developing called Consent2Share. This tool is designed to enable patient-managed granular consent, as well as the active participation of both THSA and the 12 different HIEs in Texas. Although this tool had some impressive functionalities, after much discussion was deemed not operationally feasible in the short term in Texas—in part because the tool was still in development and would require beta-testing.

The Data Work group also reviewed some of the work of the Data Segmentation for Privacy (DS4P) workgroup of ONC's Security and Interoperability (S&I) Framework. This public workgroup, which is comprised of volunteers from various constituencies like HIEs, EHR vendors, researchers, government agencies like SAMHSA and ONC, and clinicians, is developing standards, approaches, and use cases for the parsing of data into segments, the attachment of security meta-data to segments, and the alignment of patient consent with the segments. The consensus of the Data Work Group was that this work was extremely important; however, the group also acknowledged that these efforts will require a marriage of technological changes to HIEs and EHRs not likely to occur for several years, as well as changes to how consent is managed for clients. Given that the urgency the Data Work Group felt about progressing on a solution, this was not deemed to be a viable option.

After much discussion, including conversations with Texas Privacy expert Pam Beach, the Data Work Group has decided to pursue a scaled down version that, it believes, will pave the way for a complete resolution and will achieve many of the objectives of full participation with an HIE, but in a way that is consistent with obligations under §42CFR.

The Data Work Group has endorsed a two-pronged approach:

Emergency Only Consent Flag

The Data Work Group believes that the most prudent approach in the short term is to encourage THSA and HIEs in Texas do adopt an approach enabling HIEs to consume patient records with a specific consent flag indicating that the data is available on an emergency only basis. All HIEs have a provision allowing providers to "break the glass" in emergency situations to view protected patient information, and, critically, §42CFR permits the release of even substance abuse treatment information in emergency situations. Such a flag would enable all Texas Council members (with appropriate patient consent) to make all their clinical data available within an HIE.

This is a critical development that would go a long way towards addressing a host of shortcomings in the current health IT environment. To begin with, it would get HIEs accustomed to accepting the full measure of behavioral health data, particularly if they choose to adopt the additional data elements recommended by the Data Work Group. Today, there is no reliable source of healthcare data that combines behavioral health and chronic medical data other than claims data. With a substantial lag between the delivery of services and the availability of this data, however, claims data is rarely actionable at the individual care level. However, an HIE that combines behavioral health and chronic medical care would be able to prepare and deliver reports that reflect the full measure of an individual's care. Admittedly, these reports with individually identifiable health information would only be available to behavioral health agencies, but this would enable a much higher level of care coordination than exists today.

Furthermore, HIEs accepting behavioral health data with an emergency-only flag will be able to run population health reports using anonymized data that look at the intersection of behavioral health and traditional medical care. These reports could be used for a host of purposes including: community benchmarking, calculating measures for DSRIP projects, identifying trends and characteristics of high utilizers in the community, and others.

As noted above, this approach will also allow providers in emergency situations to access the full measure of patient data. A use case developed by the Data Work Group highlights how this could critically affect patient care. In this use case, a consumer with schizophrenia on clozapine presents in an emergency room with a high fever. Behavioral health data in the HIE, reviewed by a provider through a standard "break the glass" process, enables the provider to immediately cease the use of clozapine, thereby preventing a potentially fatal side effect.

Finally, with regard to future development, HIEs accepting this data with an emergency only flag starts the HIEs down the path of accepting behavioral health data. If, in the future, there are changes §42CFR requirements (for example by rescinding the "named provider" provision) or to the underlying EHR and HIE technology (for example by enabling granular segmentation and consent), the HIE will already have all of the data at its disposal. Thus, it will only require the proverbial "flip of the switch" to enable the free flow of the data. At this point, however, the only function not enabled will be the viewing of combined data by non-behavioral health providers participating in the HIE.

Exchange between Council Members

Even beyond a traditional health information exchange, Council Members have a unique need to communicate with one another regarding consumers. In this case, the providers are known specifically, enabling the sharing of full patient records including information protected by §42CFR (assuming consent is provided). To facilitate this, the Data Work Group recommends using a secure form of point-to-point information exchange such as "Direct" (the national standard for secure point-to-point exchange of individually identifiable health information), or some other secure email system that is consistent with HIPAA requirements.

Initially the DWG considered the Direct protocol alone. However, many Council Members report that they already have a secure email system enabling the exchange of sensitive information. As a result, the Data Work Group did not want to recommend duplicating services. Additionally, the Direct process—enabled for "White Spaces" in Texas through Health

Information Technology Service Providers (HITSPs)—lacked some expected functionality like a provider-look-up function. As currently executed, HITSPs allow provider look-ups only for providers participating in the same HITSP. With four different HITSPs for the white spaces alone, the DWG did not feel comfortable endorsing this as the sole approach for point-to-point exchange.

On January 17, 2014 the Texas Council Executive Directors' Consortium reviewed and approved this two-pronged approach—an emergency only flag through HIEs, and secure email for Council Member to Council Member—the DWG expects to promote exchange of clinical data and to fully comply with obligations under §42CFR part 2. What is more, this approach paves the way for a time when the regulatory and technological framework is more supportive of the appropriate exchange of sensitive health information.