

By Electronic Mail

May 23, 2011

H. Westley Clark, M.D., J.D., M.P.H., CAS, FASAM  
Director, Center for Substance Abuse Treatment  
Substance Abuse and Mental Health Services Administration  
1 Choke Cherry Road ☐  
Rockville, MD 20857

Dear Dr. Clark:

Thank you for taking time on Friday to meet with me and with my colleagues from the Software and Technology Vendors Association (SATVA) to discuss our proposed methodology to enable mental health and substance abuse providers to participate in electronic health information exchange and the National Health Information Network in a manner that ensures compliance with federal and state laws that stringently protect the privacy of sensitive health information.

Substance abuse programs are primarily concerned about compliance with 42 CFR Part 2. But as we discussed, 42 CFR Part 2 is just one of many requirements for protection of the privacy of sensitive health records that must be considered by behavioral health providers. Varying state laws restrict use and disclosure of mental health records, records of diagnosis and treatment of HIV/AIDS, genetic testing results, and other types of health information. Every clinical profession has ethical standards that require practitioners to safeguard patient privacy, and the assurance of privacy is fundamental to engagement and treatment of people with addictions or mental illness.

Privacy and data security is a particularly significant concern at this time, in light of the strong national interest in improving coordination of physical health, behavioral health, and social services to people diagnosed with mental illness or addictions, and in the use of health information technology to link services, advance the delivery of patient centered care, improve health care quality, and reduce health costs. Achievement of some level of comfort regarding compliance with privacy requirements is a prerequisite to active participation of behavioral health providers in emerging programs such as Health Homes, Accountable Care Organizations, and Regional Health Information Organizations. That participation is essential to any meaningful effort to coordinate care of high need (and high cost) individuals, who often have co-occurring physical and behavioral health disorders.

SATVA members provide software and services to support the operation of a large percentage of mental health and addiction treatment programs throughout the United States. SATVA established a workgroup to examine the legal and technical issues related to electronic health information exchange by behavioral health providers. After considerable effort, we have developed a model form of patient consent to disclosure of specifically identified health records to specific providers, and agreed to a standard method for linking that consent to health information exchange transactions. I believe that our approach addresses the requirements of 42 CFR Part 2, that it could be adapted to adhere to each state's privacy laws, and that it could be rapidly adopted and deployed throughout the United States.

Part of the reason that SATVA worked so diligently on this project is that our research did not reveal commonly accepted national standards that could be followed to inform our software development efforts.

SATVA is not wedded to a particular approach, and would welcome the opportunity to advance the adoption of any standard that has the potential to address the privacy requirements for interoperability of sensitive health records.

On Friday, you asked for a summary of the information that we provided to you and our proposal, and for a listing of issues that I had identified regarding compliance with 42 CFR Part 2 when information is exchanged through intermediary Health Information Organizations. That summary follows.

- SATVA recognizes that it is a challenge for any health care provider to understand and follow overlapping federal and state legal requirements governing electronic disclosure of health information. The FAQs issued by SAMSHA in June 2010 are helpful to the field's understanding of the application of 42 CFR Part 2 in the context of health information exchange. We are looking forward to the second set of SAMHSA FAQs on this subject.
- Anasazi is developing enhancements to its software to enable behavioral health service systems to participate in secure electronic health information exchange, and to enable creation of Personal Health Records for people served by behavioral health providers. The first use of those enhancements will be in California. A comprehensive legal analysis of the federal and state privacy and data security laws governing electronic health information exchange in California was prepared for Anasazi Software, Inc. by Paul Litwak. That analysis informed development of SATVA's proposal, and has been provided to SAMHSA.
- SATVA's proposed approach to documentation that a legally valid consent permits electronic health information exchange is designed to enable compliance with 42 CFR Part 2 as we understand it (prior to SAMHSA FAQ#2) and with state laws that are more stringent than HIPAA. It builds on existing HITSP TP-30 and HL7 3.0 communications standards for consent directive management. It offers a common mechanism for interoperability that supports point-to-point communications, communications between a Regional Health Information Organization (RHIO) and RHIO participating providers, and communications between RHIOs across the National Health Information Network. It could be rapidly deployed throughout the United States.
- For purposes of identifying the rights of individuals to control electronic disclosure of their health records, it is important to distinguish between the permissions that are legally required for:
  - (i) Any direct or indirect electronic disclosure of health information (proposed California regulations require patient consent to electronic health information exchange in addition to other legally required consents to disclosure);
  - (ii) Disclosure of individually identifiable health information to a Health Information Exchange Organization (such as a RHIO) that maintains a patient index and record locator service or a repository of health records (States have varying consent requirements. Some do not require patient consent. Others use "opt-in" or "opt-out" models. HIPAA permits covered entities to disclose protected health information to an HIEO without individual consent if there is a proper Business Associate Agreement. 42 CFR Part 2 permits disclosure without consent to an HIEO if there is a proper Qualified Services Organization Agreement.); and
  - (iii) Disclosure of health information by the holder of a record to a third party for a particular purpose (42 CFR Part 2, HIPAA, and State privacy laws).

- HIPAA permits disclosure of protected health information other than psychotherapy notes to a health care provider for treatment purposes without patient consent.
- With limited exceptions, patient consent is required before a federally assisted substance abuse program may provide any patient identifying information to a third party for any purpose, including treatment. The holder of a record protected by 42 CFR Part 2 may not provide any information that would indicate that an identifiable individual has received treatment at the substance abuse program. The required elements of a consent are set forth at 42 CFR 2.31. The consent must identify the name of the patient, the specific name or general designation of the program or person permitted to make the disclosure, the recipient of the record, the purpose of the disclosure, and how much and what kind of information will be disclosed. It must state that the consent may be revoked, and establish a date or event upon which it will expire.
- Similar forms of consent are required in individual states that stringently control disclosure of specific types of health records. For example, the State of Maine requires patient consent to all disclosures of mental health records, and specifies the form of consent. (Maine Revised Statutes, Title 22, Section 1711-C).
- The SATVA workgroup endorses use of a standard Consent Form to permit an identified holder of a health record to disclose health information to an identified third party. The form should include the “lowest common denominator” of elements required by federal and state laws governing disclosure of sensitive health information (such as substance abuse program records, HIV records, etc.) Slightly different forms would be used in different States, but the common elements would remain the same.
- The legal analysis provided to Anasazi concludes with a Model Form of Consent to Electronic Health Information Exchange for use by Behavioral Health Providers in California. The Model Consent Form includes the elements required by 42 CFR 2.31, the California Confidentiality of Medical Information Act, and proposed California regulations governing electronic health information exchange.
- The Model Consent form permits electronic exchange of health information held by one identified provider to another identified provider for treatment purposes only. This approach is consistent with the NHIN-Direct communications standards for communications between known, trusted providers. The form is written in a manner that limits use of free text or incalculable dependencies so as to facilitate automation of the process of recording and tracking permission to disclose records.
- It seems to be premature to attempt to implement granular controls over disclosure of specific classes of data included within an individual clinical record. A “Privacy and Security Tiger Team” assembled by the Office of the National Coordinator for Health Information Technology recently examined this issue and reported that while granular consents are desirable, there is no current standard for implementation of such controls in EHR systems, and that the vast majority of individuals who are offered the opportunity to exercise granular consent control refuse the opportunity and give a general consent to disclose the entire health record. The model consent form has therefore been designed to apply to the entire record.
- Please note that it would be possible to create a 42 CFR Part 2 compliant consent form that permits disclosure of a substance abuse program record to a set of identified recipients and that permits those recipients to re-disclose the information in the record to one another. This would facilitate electronic

health information exchange among an identifiable and unchanging group of providers. But it would not be a practical approach to consent directive management in the context of the National Health Information Network because it is not scalable beyond limited communities of identified providers.

- SATVA proposes the use of a standard HITSP TP-30 HL 7 3.0 transaction to communicate Consent Directives. One or more Health Information Services Providers (HISPs) would: (i) authenticate the identity of the providers that participate in the health information exchange transaction; (ii) establish that a trust relationship exists (through reference to a DURSA or other standard NHIN participation agreement); (iii) confirm that the patient has given the legally required form of consent to disclose the particular record to the receiving provider. (This consent could be given by the patient through a Personal Health Record, or obtained by the sending provider or the receiving provider); and (iv) transmit an encrypted health record from the sending provider to the receiving provider. The TP-30 “wrapper” around the health record would include all legally required notices to the recipient regarding further re-disclosure of the record. Regional Health Information Organizations could play the role of HISP, in addition to providing patient identifier, record locator, health data repository, or patient portal services.
- A Regional Health Information Organization or other entity that acts as an intermediary between providers for purposes of facilitating health information exchange could be considered to be providing a service to participating providers to enable them to exchange information through the National Health Information Network. Pursuant to the HITECH Act, Health Information Exchange Organizations (including RHIOs) are a business associate of the provider organizations that use the HIEO to facilitate the exchange of data. HIPAA covered entities that enter an appropriate Business Associate Agreement with the HIEO may disclose patient records to the HIEO without individual consent or authorization.
- A Health Information Exchange Organization could also be considered a “Qualified Service Organization” that provides services to federally qualified substance abuse programs. This would permit a substance abuse program that enters an appropriate Qualified Services Organization Agreement with the HIEO to disclose records to the HIEO. It would not permit the HIEO to re-disclose the record to third parties.
- The standard agreements between federally assisted substance abuse programs and RHIOs or other Health Information Exchange Organizations should include the provisions required for HIPAA Business Associate Agreements and Qualified Service Organization Agreements. These provisions overlap, and could be incorporated into one document.
- The Data Use and Reciprocal Support Agreement (DURSA) that governs the exchange of health data through the National Health Information Exchange Network (NHIN) should obligate Health Information Exchange Organizations to comply with 42 CFR Part 2 when they receive individually identifiable records from federally assisted substance abuse programs.
- Please contrast the approach to consent directive management recommended by SATVA (using a standard Consent Form that complies with 2.31) with the forms used by the Veteran’s Administration and New York State RHIOs to secure patient permission to disclose health information.
  - (i) Veteran’s Administration records are not subject to 42 CFR Part 2. But it is worth noting that the Veteran’s Administration Health System in San Diego is implementing a “Virtual Lifetime

Electronic Record” and using VA Form 10-0485 to obtain patient authorization of disclosure for treatment purposes of all VA health records (including sensitive records such as treatment for alcohol or drug abuse) “to the communities that are participating in the Nationwide Health Information Network”. The recipient of the record is not specified.

- (ii) In New York State, the eHealth Collaborative has established Privacy and Security Policies and Consent Forms for use by Regional Health Information Organizations and their participants. The NY Consent Form permits a specific health care provider to receive any health information that may be available through the RHIO. This includes sensitive information such as records of mental health or substance abuse treatment, HIV status, and genetic testing results. SAMHSA has not given an opinion as to whether such a form of permission to receive health records through a RHIO meets the requirements of 42 CFR 2.31.
- Federated, Repository, and Hybrid RHIOs generally provide a Record Locator Service that allows a Participant to find all other Participants of that RHIO that have treated a particular Consumer and can often identify the nature of the information in the record or the provider type or specialty. Except in a bona fide medical emergency, 42 CFR Part 2 prohibits display of the fact that a Consumer has been treated at a provider known to be a 42 CFR Part 2 Program unless the Consumer has specifically permitted the RHIO Participant that holds the record to disclose that information to the RHIO Participant (and its Users) that submitted the query.
  - When substance abuse program records are disclosed with patient consent, a written notice must be sent to the recipient of the information advising the recipient that the record is protected by 42 CFR Part 2, that the recipient is obligated to follow those regulations, and that re-disclosure of the information provided is prohibited without the express permission of the patient or as permitted by 42 CFR Part 2. The form of that notice is specified at 42 CFR 2.32. This notice would be required whenever a Record Locator Service or Patient Portal provided by a RHIO provides information that associates an individual with a record of a federally assisted substance abuse program.
  - SATVA recommends that an electronic consent directive transaction accompany electronic transactions containing sensitive health records. The electronic consent directive transaction would contain a structured data element that notifies the recipient that re-disclosure of the information provided in the transaction is prohibited.
  - Substance abuse program records may be disclosed without patient consent in a medical emergency. But immediately following the disclosure, the disclosing organization must document the disclosure in the patient’s record, setting forth the identity of the medical personnel and health care facility that received the record, the name of the individual making the disclosure, the date and time of disclosure, and the nature of the emergency. Health Information Exchange Organizations that support “break the glass” procedures to enable emergency disclosures without consent must be able to support this requirement. The HIEO should provide a mechanism to electronically report the required information to the 42 CFR Part 2 program in a structured format so that the program can incorporate that information in the patient’s electronic health record. SATVA recommends exploring whether this information could be reported in a TP-30 transaction.

Once again, Dr. Clark, thank you for your time and attention to these important issues. I look forward to continuing to work with you and with your colleagues at SAMHSA, ONC, and OCR. I can be reached at 800-651-4411 and ask for my assistants Andrea or Jessica or by email to [mmorris@anasazisoftware.com](mailto:mmorris@anasazisoftware.com).

Sincerely,

A handwritten signature in black ink, appearing to read "Michael Morris". The signature is fluid and cursive, with the first name "Michael" and last name "Morris" clearly distinguishable.

Michael Morris  
CEO  
Anasazi Software, Inc.