HHS Issues Revised Rule on Confidentiality of Substance Abuse Record

Insights 01.25.17

PROFESSIONAL

AMY M. JOSEPH
Partner
Boston

STEPHEN K. PHILLIPS
Partner
San Francisco

ROBERT L. ROTH
Partner
Washington, D.C.

PAUL T. SMITH
Partner
San Francisco

The federal Substance Abuse and Mental Health Services Administration has published a final rule on the confidentiality of substance abuse records. The rule is intended to update and modernize the existing regulations and facilitate information exchange within new health care models. It is available here. The regulation goes into effect February 17, 2017. At the same time, SAMHSA published a proposed regulation to clarify aspects of the new rule.

This is the first significant update of these regulations since 1987. Much has changed since then, including the development of new health care models that require information exchange, and new methods of exchanging health information. SAMHSA wants to ensure that patients with substance use disorders can participate in improvements in health care delivery without compromising the privacy of their health information. It has done this by enhancing information security requirements, and by permitting disclosure of patient information through intermediaries such as ACOs and health information exchanges with patient consent. Patients whose information is disclosed through third parties are entitled to an accounting of these disclosures.

Instead of "alcohol and drug abuse" the affliction is now called "substance use disorder." The revised regulations use the same general approach as the existing ones: Federally assisted substance use disorder programs – now called part 2 programs – are prohibited from using or disclosing patient identifying information, whether or not recorded, that would identify a patient as having or having had a substance abuse disorder, unless the regulations provide an exception or the patient consents.

DEFINITIONS

There is a new definition of "substance use disorder": it means a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal. The definition does not, however, include tobacco or caffeine use.

The definition of "disclose" is broader now – it means to communicate any information identifying a patient as being or having been diagnosed with a substance use disorder, having or having had a substance use disorder, or being or having been referred for treatment of a substance use disorder either directly, by reference to publicly available information, or through verification of the identification by another person. The current regulations state that they do not restrict a disclosure that an identified individual is not and never has been a patient. This is deleted in the new rule – SAMHSA says to mitigate against fishing by third parties.

The definition of "patient" now includes someone who has applied for a referral for treatment for a substance use disorder, as well as someone who has been diagnosed with or treated for a disorder, and includes both current and former patients, living or deceased.

The definition of "Patient identifying information" is unchanged – it means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient can be determined with reasonable accuracy either directly or by reference to other information. The regulation permits the disclosure of de-identified information, if identifiers are removed to create a "very low risk" of re-identification. This is similar to the HIPAA rule, which requires a "very small" risk of re-identification; but unlike HIPAA, this rule has no safe harbor method of de-identification.

The definition of "Records" is amplified to include any information, whether recorded or not, created by, received, or acquired by a part 2 program relating to a patient (e.g., diagnosis, treatment and referral for treatment information, billing information, emails, voice-mails, and texts). Records include both paper and electronic records.

The regulation does not widen the scope of covered programs – these remain:

- An individual or entity (other than a general medical facility) that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
- An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
- Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

The regulations apply also to third party payers, entities that have direct administrative control over part 2 programs, and anyone else who receives patient records directly from a part 2 program or another holder of the information and is notified of the prohibition on re-disclosure.

As presently, the revised regulation covers only federally assisted programs. What it means to be federally assisted is largely unchanged, except that the list is expanded to include all federally-authorized maintenance treatment and withdrawal management programs (and there are new definitions for these).

EXCEPTIONS

Communications for diagnosis, referral and treatment. The regulations keep the principal exception, which allows communications for diagnosis, referral or treatment within a part 2 program or between a part 2 program and an entity that has direct administrative control over the program.

Contractors. The rule permits communications between a part 2 program and a qualified service organization providing services to the program, if the recipient signs an agreement to be bound by the regulations. The definition of "qualified service organization" is expanded to include organizations that provide population health management or medical staffing services to the program. The proposed rule issued concurrently with the new final rule would allow a patient consent to permit additional disclosures of the patient's health records for payment and health care operations (the list of permitted activities is similar to the HIPAA list, but not as broad) . Such a consent would then permit the program to disclose the records minimally necessary for its contractors and legal representatives to carry out a range of activities related to payment and health care operations. The program would be required to have an agreement with its contractors binding them to the regulations, specifying the purposes for which they may use the information, restricting re-disclosure, and requiring them to safeguard the information and report unauthorized uses and disclosures to the program – in short, a kind of business associate agreement.

Medical Emergencies. The exception for disclosure without consent in medical emergencies has been broadened to give programs more discretion to determine when an emergency exists: it now permits disclosure to medical personnel to the extent necessary to meet a *bona fide* medical emergency in which the patient's prior informed consent cannot be obtained. The regulation retains the requirement for immediate documentation of the disclosure and the reasons for it.

Research. The rule expands the use of part 2 program records for scientific research. It allows any lawful holder of part 2 program information (not just the program itself) to disclose protected information to qualified personnel for the purpose of conducting scientific research if the researcher provides documentation that it meets the requirements of HIPAA or the HHS Common Rule governing research on human subjects (or both, if both are applicable). Researches receiving protected information under these provisions are fully bound by the rule, and may include program data in their research reports only in aggregate, non-identifiable form.

The rule also allows researchers holding protected data to obtain linkages to federal and non-federal data repositories that include patient identifying information if the data linkage component is reviewed and approved by an IRB registered with HHS's Office for Human Research Protection.

Audit and evaluation. The rule updates the audit and evaluation requirements to include provisions for both paper and electronic patient records, and to permit audits and evaluations necessary to meet the requirements of Medicare accountable care organizations or similar CMS-regulated organizations under certain conditions. The recipient – such as an ACO – must agree to maintain and destroy the patient identifying information in a manner consistent with the new security requirements of the rule; retain records in compliance with applicable federal, state, and local record retention laws; and limit use to its audit functions, and its disclosures to the program that provided the information. The regulation also contains administrative, operational and oversight requirements for ACOs that receive program information.

The final rule allows disclosure for audit and evaluation purpose only to Medicare ACOs and similar entities regulated by CMS. Commenters had noted that a variety of entities may perform audit and evaluation activities for private payers, as well as the Medicare and Medicaid programs. The proposed rule issued concurrently with the final rule would expand this exception to cover anyone who provides financial assistance to a part 2 program, third-party payers covering patients in a part 2 program, and quality improvement organizations performing a utilization or quality control review for a part 2 program.

Other exceptions. Other exceptions remain in place without significant changes, including those for reporting crimes on program premises or against program personnel, and reporting suspected child abuse and neglect.

INFORMATION SECURITY

The regulations expand the security requirements for program information. The program or other holder of patient information must have in place formal policies and procedures to protect against unauthorized uses and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information. These formal policies and procedures must address:

Paper records, including:

- Transferring and removing records;
- Destroying records, including sanitizing the hard copy media associated with the paper printouts, to render the patient identifying information non-retrievable;
- Maintaining records in a secure room, locked file cabinet, safe, or other similar container, or storage facility when not in use;
- Controlling access to accessing workstations, secure rooms, locked file cabinets, safes, or other similar containers, and storage facilities that use or store such information; and
- De-identifying records. Records that have been rendered non-identifiable in a manner that creates a "very low risk" of re-identification is not protected.

Electronic records, including:

- Creating, receiving, maintaining, and transmitting electronic records;

- Destroying records, including sanitizing the electronic media on which electronic records are stored, to render the patient identifying information non-retrievable;
- Using and accessing electronic records or other electronic media containing patient identifying information; and
- De-identifying electronic records.

Policies and procedures that comply with the HIPAA Security Rule should address these topics.

The regulations contain new provisions for the destruction of records of programs that are discontinued, and for ensuring the security of records that state or other law requires a discontinued program to maintain.

PATIENT NOTICE AND CONSENT

Patient notice. The regulations require programs to give patients a written summary of the federal law and regulations. The new regulation clarifies that the notice may be in paper or electronic form. It must now contain contact information for reporting violations of the rule to the appropriate authorities. The former regulation had a sample notice, which has been removed from the revised regulation.

Patient Consent. Written consent of the patient is required for disclosures not otherwise permitted. The revised regulation clarifies that the consent may be paper or electronic, and expands the requirements for a valid consent. These are similar now to those of a HIPAA authorization, with some additional restrictions:

- The consent must contain an explicit description of the substance disorder information that may be disclosed (HIPAA allows a general description).
- The consent must contain the names of the individuals or entities to whom the disclosure is to be made (HIPAA allows a description without specific names). If the recipient does not have a treatment relationship with the patient and is not a third-party payer (for example, if the recipient is an ACO, a health information exchange or a research institution), the consent may state the names or a general description of participants that have treating provider relationships with the patient whose information is being disclosed, and disclosure may be made to these providers (but not to anyone else who is not designated by name). This is referred to as a general designation; an example is "my current and future health care providers." A consent that uses a general designation must include a statement that the patient is entitled to a list of entities to which the information has been disclosed pursuant to the general designation. This right covers disclosures made within two years preceding the request. The intermediary entity (not the part 2 program) is responsible for responding to the request; it must do so within 30 days of the request, providing the names of the entities to which disclosure was made, the date of the disclosure, and a brief description of the patient information disclosed. Intermediaries may not disclose information pursuant to a general designation until they have the capability to provide list of disclosures. In this respect the final regulation is stricter than the proposed rule, which would have allowed two years to comply with the disclosure requirement.
- The consent may not last longer reasonably necessary to serve the purpose for which it is provided (HIPAA requires authorizations to be limited in time, but does not prescribe a limit).

In addition, the recipient of the information must be given a written notice that the information is protected by the federal confidentiality rules (42 CFR part 2), which prohibit further disclosure of the information.

Hooper, Lundy & Bookman provides a range of legal services relating to health information privacy, security and technology. For more information, please contact: In San Francisco, Paul Smith or Steve Phillips; in Los Angeles, Hope Levy-Biehl; in Washington, D.C., Bob Roth; or in Boston, Amy Joseph.

RELATED CAPABILITIES

Health Information Privacy and Security