Best Practices in Navigating HIPAA and 42 CFR Part 2: A Client, Family and Organizational Perspective

Gerald (Jud) E. DeLoss, J.D.
Chief Executive Officer/General Counsel
Illinois Association for Behavioral Health

July 30, 2020

SAMHSA
Substance Abuse and Mental Health Services Administration

Disclaimer Slide

This webinar was developed [in part] under contract number HHSS283201200021I/HHS28342003T from the Substance Abuse and Mental Health Services Administration (SAMHSA), U.S. Department of Health and Human Services (HHS). The views, policies and opinions expressed are those of the authors and do not necessarily reflect those of SAMHSA or HHS.

SAMHSA
Substance Abuse and Mental Health Services Administration

Overview of Today's Presentation

- Summary of key Health Insurance Portability and Accountability Act (HIPAA) provisions
- Overview of Confidentiality of Substance Use Disorder Patient Records regulations, 42 CFR Part 2 (Part 2)
- Practical tips to include family and caretakers in health care decision making
- How patients may control their information and limit who can access and what
- Steps that providers may implement to ensure patient and caretaker engagement and comply with HIPAA and Part 2

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA

- Right of Access
  - Patient has right to request copy of or review of medical records
- Right of Amendment
  - Patient may request an amendment to their medical record
  - Provider may refuse request
  - If refused, patient may still request a statement be included in the medical record explaining disagreement (provider may include their response)
- Right to Request Accounting
  - Patient may request listing of certain disclosures over prior six years
- Right to Request Confidential Communications
  - Patient may request communication in alternative means
  - Provider must accept if reasonable
- Right to Request a Restriction
  - Patient may request that information not be disclosed
  - Provider only required to comply with request if related to disclosure to health plan for item paid in full out of pocket

HIPAA

- Sharing of information with family, friends, and designated individuals
- Including family and others in health care discussions and treatment
- Examples:
  - A doctor may give information about a patient's condition to a friend driving the patient home
  - A hospital may discuss a patient's payment options with an adult son or daughter
  - An advanced practice nurse may instruct a patient's roommate about proper medicine dosage
  - A physician may discuss a patient's treatment with the patient in the presence of a friend when the patient brings the friend to the examination room during a medical appointment

HIPAA

- Sharing of health information with family members, friends, and caretakers
  - Permitted under HIPAA if in the professional judgment of the provider you would not object and in your best interests
- Permits covered entities to notify, or assist in the notification of, family members, personal representatives, or other persons responsible for the care of the patient, of the patient's location, general condition, or death

HIPAA

- Revoking the covered entity's ability to share information with family members, friends, and caretakers
- Objection by patient is sufficient for specific situation
- General notification would need to be included in medical record
  - Best practice to advise covered entity at each interaction
- Request to provider not to disclose to health plan for payment of item or service paid in full out of pocket must be followed by provider

HIPAA

Personal Representative

- A person is an individual's personal representative if, under applicable state law, he or she can act on the individual's behalf in making decisions related to health care
- Examples:
  - Health Care Power of Attorney
  - Guardianship
  - Parent of unemancipated minor
    - Depends upon authority of the minor to act to make health care decisions
  - Executor of estate of the deceased

HIPAA

Steps that providers can take to ensure patient and caretaker engagement

- Implement policies that recognize importance of family, friend, and caretaker involvement in health care and treatment
- Require verbal confirmation of agreement of patient to permit third parties to participate in treatment or discussion – even in situations in which lack of objection is acceptable under HIPAA
- Document patient agreement/lack of objection in the medical record
- Share the benefits of including friends, family, and caretakers in treatment, decisions, and payment
- Personal representatives should be able to provide documentation supporting their status and verification of the identity and authority
    - Provider should verify identity and authority with documentation

42 CFR Part 2 - Confidentiality of Substance Use Disorder Patient Records

SAMHSA
Substance Abuse and Mental Health Services Administration

Part 2

- Confidentiality of Substance Use Disorder (SUD) Patient Records regulations are under 42 CFR Part 2 or “Part 2”
- Applies to federally-assisted SUD treatment facilities
- Applies to **all** recipients of SUD patient records – not just treatment facilities
- Generally, Part 2 is much more stringent than HIPAA for uses and disclosures of SUD patient records
- Patient consent is usually required for most uses and disclosures, including those for treatment, payment, and health care operations – which HIPAA permits without authorization
- Disclosures to family, friends, and caretakers generally prohibited without express patient consent
- Limitations apply so far as to prohibit disclosure of presence in facility – name may not be used without consent

Part 2

- Modifications to statutory basis for Part 2 under the CARES Act
- Brings privacy protections for substance use disorder records into alignment with privacy protections for general medical treatment and related records under the Health Insurance Portability and Accountability Act (HIPAA)
  - Requires general consent for disclosure of substance use disorder treatment records
  - Allows disclosure of covered records for treatment, payment and operations
  - May be redisclosed in accordance with HIPAA
- Applies to Part 2 Programs, covered entities, and business associates
- Allows for disclosure of de-identified substance use disorder records to public health authorities
- Prohibits use of protected substance use disorder records in civil, criminal, legislative, or administrative proceedings other than by Court order or patient consent
- New, increased penalties for violation of the protections under authority of HHS/OCR
- Obligation to notify HHS/OCR of breaches
- Protections against discrimination based on intentional or inadvertent disclosure of covered records

Part 2

- Part 2 Programs must still obtain consent in order to disclose
  - Uses and disclosures only for treatment, payment, and certain health care operations
- SUD records will still need to be segregated from other patient records to track consent and disclosure
  - Initial disclosure and downstream disclosures
- Amended law imposes stronger enforcement provisions and penalties
  - Enforcement will be overseen by the HHS Office for Civil Rights (“OCR”), which oversees HIPAA enforcement
- Increased protection of SUD records from use in civil, criminal, administrative, and legislative proceedings
- Accounting of disclosures requirement under HITECH Act now applies
- Right of individual to request restriction on use or disclosure under HITECH Act

Part 2

- Consent
  - Must be obtained prior to disclosure
  - Must be in writing
  - May obtain consent once for all future uses or disclosures until revoked

Part 2

Provider Concerns

- Likely further increased emphasis on collection of consent forms
  - Initial consent required by covered entities, business associates, and Part 2 programs
- Multi-specialty providers need to distinguish between internal operations that constitute Part 2 programs from those that do not
  - Will still need initial consent to share among various departments or service lines
- Distinguish between disclosures for treatment, payment, and operations and other disclosures
  - Not all health care operations purposes are permissible (fundraising, de-identified information, limited data sets)

Part 2

- Model notice to be issued by the Secretary not later than 1 year after enactment of the CARES Act
  - Must be easily understandable and in plain language
  - Must include:
    - a statement of the patient's rights with respect to protected health information (including for self-pay patients)
    - a brief description of how the individual may exercise their related rights and
    - a description of each purpose for which the covered entity is permitted or required to use or disclose protected health information without the patient's written authorization

Part 2

- Breach – the acquisition, access, use, or disclosure of protected health information in a manner not permitted under applicable regulations which compromises the security or privacy of the protected health information.
  - Disclosure in a manner not permitted by regulations is presumed to be a breach, unless
    - good faith but unintentional acquisition, access or use by workforce member or person under the authority of a covered entity or business associate if no unpermitted use or disclosure
    - Inadvertent disclosure by and to person with authorized access at covered entity or business associate if no further unpermitted use or disclosure
    - Covered entity can demonstrate through risk assessment that there is a low probability that the protected health information has been compromised

Part 2

- In case of a breach, covered entity must notify each individual whose unsecured protected information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of such breach.
  - Business associates notify covered entities of breach
- Breach is considered discovered as of the first day on which it is known to the covered entity, or by which the covered entity would have known had it exercised reasonable diligence
- Must notify patient without unreasonable delay and no more than 60 calendar days after discovery
- Notice must be written in plain language and must include, to the extent possible:
  - Brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  - Description of the types of unsecured protected health information involved in the breach (e.g., full name, SSN, DOB, home address, account number, diagnosis, disability code, etc.);
  - Steps individuals should take to protect themselves from potential harm resulting from the breach;
  - Brief description of the covered entity s actions to investigate the breach, mitigate harm to individuals, and protect against further breaches;
  - Contact procedures for questions or additional information
- Must notify HHS within 60 days if 500 or more individuals; within 60 days of end of calendar year for others
- Must notify media if more than 500 individuals in state or jurisdiction

Part 2

- The legislation introduces explicit protections against discrimination based upon Part 2 records or information about the patient disclosed under Part 2 – either inadvertently or intentionally. Specifically, no entity may discriminate against a patient about whom the Part 2 records relate in:
  - Admission, access to, or treatment for health care
  - Hiring, firing, or terms of employment, or receipt of worker's compensation
  - Sale, rental, or continued rental of housing
  - Access to Federal, State, or local courts
  - Access to, approval of, or maintenance of social services and benefits provided or funded by Federal, State, or local governments
- No recipient of Federal funds may discriminate against the patient based upon the Part 2 records in affording access to the services provided with such funds

Part 2

- The prohibition against discrimination for health care raises interesting questions about organ donation, or participation in research studies
- The prohibition against discrimination in employment raises additional questions regarding the use of illegal substances, medical marijuana, and permitted recreational marijuana in the workplace or while on call
- Other questions include impact in abstinence-only treatment programs and supported housing conditions for recipients

Part 2

- Except with a valid court order or patient consent, Part 2 records or testimony about such records may not be disclosed or used in any civil, criminal, administrative, or legislative proceeding conducted by any Federal, State, or local authority, against a patient, including that:
- The record or testimony shall not be entered into evidence in any criminal prosecution or civil action before a Federal or State court
- The record or testimony shall not form part of the record for decision or otherwise be taken into account in any proceeding before a Federal, State, or local agency
- The record or testimony shall not be used by any Federal, State, or local agency for a law enforcement purpose or to conduct any law enforcement investigation
- The record or testimony shall not be used in any application for a warrant

Part 2

- Expands existing protections beyond just civil or criminal proceedings
- Disclosures to third parties for these purposes would not likely fall under Treatment, Payment, or Health Care Operations
- Maintains traditional Part 2 “downstream” protections
- Would appear to take away subpoena and compulsory processes held by administrative agencies and legislative bodies – as only “court” order may compel disclosure

Part 2

- Part 2 has historically been enforced criminally by the US Attorney (42 C.F.R. § 2.4) and penalties under Title 18 of the U.S. Code (42 C.F.R. § 2.3)
- Penalties now set forth under sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d–5 and 42 U.S.C. 1320d–6), which are the penalties imposed for HIPAA violations
- Penalties for civil violations
  - HIPAA violation: Unknowing - Penalty range: $100 - $50,000 per violation, with annual maximum of $25,000 for repeat violations
  - HIPAA violation: Reasonable Cause - Penalty range: $1,000 - $50,000 per violation, with annual maximum of $100,000 for repeat violations
  - HIPAA violation: Willful neglect but violation is corrected within the required time period - Penalty range: $10,000 - $50,000 per violation, with an annual maximum of $250,000 for repeat violations
  - HIPAA violation: Willful neglect and is not corrected within required time period - Penalty range: $50,000 per violation, with an annual maximum of $1.5 million
- Criminal penalties
  - “Knowingly" obtain or disclose individually identifiable health information, in violation of the Administrative Simplification Regulations, face a fine of up to $50,000, as well as imprisonment up to 1 year
  - Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to 5 years in prison
  - Offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000 and imprisonment up to 10 years

Part 2

It is the sense of the Congress that—

(1) Any person treating a patient through a Part 2 program or activity with respect to which the SUD confidentiality requirements apply is encouraged to access the applicable State-based prescription drug monitoring program when clinically appropriate

(2) Patients have the right to request a restriction on the use or disclosure of a SUD record for treatment, payment, or health care operations

(3) Covered entities should make every reasonable effort to the extent feasible to comply with a patient's request for a restriction regarding such use or disclosure

(4) For purposes of SUD confidentiality protections, “health care operations “ shall have the meaning given such term in the HIPAA regulations except that this term shall not include the creation of “de-identified health information or a limited data set, and fundraising for the benefit of the covered entity”

(5) Programs creating protected SUD records should receive positive incentives for discussing with their patients the benefits to consenting to share such records

Questions?

Gerald (Jud) E. DeLoss, J.D.
Chief Executive Officer/General Counsel
Illinois Association for Behavioral Health
jud@ilabh.org
217.528.7335

SAMHSA
Substance Abuse and Mental Health Services Administration