Testimony of Gerald (Jud) E. DeLoss

Greensfelder Hemker & Gale P.C.
Chicago, IL

Before the House Energy & Commerce Committee
Health Subcommittee

Improving the Coordination and Quality of Substance Use Disorder Treatment

May 8, 2018

My name is Gerald (Jud) E. DeLoss and I am a partner with the law firm of Greensfelder, Hemker & Gale, P.C. in Chicago, Illinois. I am a health law attorney that focuses on health information privacy and confidentiality and behavioral health law. I have extensive experience with HIPAA and 42 C.F.R. Part 2 (Part 2). I have previously served as the Chair of the Health Information & Technology Practice Group of the American Health Lawyers Association (AHLA) and Chair of the Behavioral Health Task Force of the AHLA. I represent several substance use disorder (SUD) treatment programs covered by Part 2 and other behavioral health provider clients including Lake County, NICASA, North Central Behavioral Health Systems, Stepping Stones Treatment Center, and TASC. I am here today on behalf of Netsmart Technologies, a technology partner to behavioral health, substance use treatment, and post-acute providers nationwide.

I am here today to explain the existing protections under the Health Insurance Portability and Accountability Act of 1996 and the Privacy and Security Regulations promulgated thereunder (jointly "HIPAA") and Part 2 and the protections that would remain in place following

enactment of HR 3545 and HR 3545 as amended. I believe there have been misstatements of the law and the protections they provide. My testimony is intended to provide a correct summary of the law and clear up any misunderstandings of the substantial protections in place for the privacy of SUD patient records.

Limited Impact of HR 3545 on Part 2

At the outset it is important to note that the Bill only modifies uses and disclosures of Part 2 SUD patient information for purposes of "treatment", "payment", and "health care operations", each as defined under HIPAA. The Bill does not reduce or remove Part 2 protections against disclosures to employers, landlords, life insurance companies, or in response to subpoenas or discovery requests. Those disclosures are not "TPO" (Treatment, Payment, and health care Operations) as defined by HIPAA. Those disclosures would still be governed by, and protected by, Part 2.

Furthermore, the amended Bill only allows for disclosure "[t]o a covered entity by a covered entity, or to a covered entity by a [Part 2] program" for purposes of TPO. Under HR 3545, as amended, the only disclosures authorized for TPO would be to covered entities, which under HIPAA only include certain health care providers, health plans, and health care clearinghouses. Disclosures to third parties that are not considered HIPAA covered entities would not be allowed. Employers, landlords, life insurance companies, marketers, and the courts are not covered entities. Disclosure to those entities or individuals would not be allowed under the amended Bill.

The definition of “treatment” under HIPAA would allow for the disclosure of health information to a covered entity or a health care provider. Under HR 3545 as amended, health information cannot be disclosed to a health care provider. The disclosure of health information is only permitted to a covered entity. The definition of “payment” under HIPAA would allow for disclosures to third parties for reimbursement and payment-related purposes. Under HR 3545 as amended, health information cannot be disclosed to third parties unless they are HIPAA covered entities. The definition of “health care operations” encompasses many functions and allows for sharing of health information to a variety of third parties. Under HR 3545 as amended, health information cannot be disclosed to third parties – only covered entities. Because health information may only be disclosed to covered entities under HR 3545 as amended, there is no ability for the information to be shared or re-disclosed by a Part 2 program or covered entity to any other recipient unless the recipient is a covered entity. Covered entities would be bound by HR 3545 as amended, by HIPAA, and could not disclose or re-disclose the health information to any other third party, except for other covered entities.

HR 3545 as amended would also not expressly allow for disclosures to or by HIPAA business associates, which are third parties that carry out distinct operations and tasks for covered entities. Disclosures are only permitted to a covered entity. Part 2 allows for disclosures necessary for operations or similar purposes to contractors or agents of the Part 2 program, which are defined as qualified service organizations.[1] Any such disclosures to the qualified service organizations would need to be carried out utilizing a qualified service organization agreement (QSOA) pursuant to Part 2.

[1] 42 CFR § 2.11.

The proponents of maintaining the old Part 2 configuration argue that the Bill will open the floodgates and "eviscerate" the protections available under the law. However, they fail to mention two critical items. First, the Bill only allows for uses and disclosures for treatment, payment, and health care operations purposes as defined under HIPAA. These types of uses and disclosures are typical in the health care world. For example, when a patient is being admitted to treatment, a Part 2 program will require consent to share information with the patient's insurance company to coordinate benefits and ensure reimbursement. Part 2 provides that a program need not admit a patient until assurances of reimbursement are in place. These types of disclosures are limited, purposeful, and necessary for our health care system to operate. Second, those disclosures relating to life and disability insurance, family law and custody disputes remain unchanged and under the Bill will still require patient consent or a court order.

Legal Protections Provided by HIPAA

In addition to the limitations on disclosures set forth in HR 3545, HIPAA provides stringent protections against the use of health information by employers, for child custody determinations, and by law enforcement. Like Part 2, HIPAA generally prohibits the disclosure of health information to third parties without patient authorization or court order. The arguments advanced by those who support continuing the existing regulations do not take into consideration the stringent legal protections already available under HIPAA and the robust enforcement of HIPAA that dwarfs the little – to no – enforcement that has been undertaken with respect to Part 2.

Minimum Necessary Protections under HIPAA

Under HIPAA, disclosures of health information for payment and operations purposes must utilize the minimum amount of health information that is required in order for the parties to process and pay for claims or engage in the operation.[2] Further, providers are required by HIPAA to develop and implement policies and procedures that appropriately limit the use and disclosure of health information to the minimum necessary to accomplish the intended purpose, such as obtaining payment from a health insurer for services rendered.[3] These minimum necessary requirements are in place to limit the amount and type of information shared for non-treatment contexts, reducing the likelihood and impact of any breach or loss of data.

Employment Protections under HIPAA and ADA

As explained above, the disclosure of health information to an employer would not be considered part of TPO. Any disclosure to an employer under HIPAA would be governed by specific regulations that generally prohibit the disclosure of health information to an employer without an authorization or court order. Under HIPAA, the health care provider must provide the health care service to the individual at the request of his or her employer or as a member of the employer's workforce. The health care service provided must be for medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related injury. Further, the employer must have a duty under the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or the requirements of a similar State law, to keep records on such information.[4] Even in that limited situation, the employer must request

---

[2] 45 CFR §§ 164.506(c) and 164.502(b).
[3] 45 CFR § 164.514(d)(3).
[4] 45 CFR § 164.512(b)(1).

the evaluation, and the healthcare provider must provide advance written notice to the patient.[5] In addition, employers who sponsor group health plans are prohibited from using or disclosing health information for employment-related decisions or any other benefit decision.[6]

Generally, under the Americans with Disabilities Act ("ADA"), an employee whose poor performance or conduct is attributable to an SUD may be entitled to a reasonable accommodation and the employer cannot discriminate against the employee based upon the SUD, which is considered a disability. The ADA will not allow for an employee to engage in the use of substances while at work, if the employer prohibited such illegal use. As a result, an employer does not violate the ADA by uniformly enforcing its rules prohibiting employees from illegally using drugs on the job or in the workplace.[7] However, "qualified individuals" under the ADA include those individuals:

- Who have been successfully rehabilitated and who are no longer currently engaged in the illegal use of drugs[8]
- Who are currently participating in a rehabilitation program and are no longer currently engaging in the illegal use of drugs[9]
- Who are regarded, erroneously, as currently illegally using drugs[10]

An individual suffering from an SUD may be protected under the ADA because the addiction may be considered a substantially limiting impairment.[11]

---

[5] Id.
[6] 45 CFR § 164.504(f)(2)(ii)(C). In addition, the group health plan documents must restrict uses or disclosures to those specifically permitted under 45 CFR § 164.504(f). See 45 CFR § 164.504(f)(1).
[7] EEOC Technical Assistance Manual on the ADA § 8.3.
[8] 42 U.S.C. § 12114(b) (1994).
[9] 42 U.S.C. § 12114(b) (1994). A "rehabilitation program" may include inpatient, outpatient, or employee assistance programs, or recognized self-help programs such as Narcotics Anonymous. EEOC Technical Assistance Manual on the ADA § 8.5.
[10] 42 U.S.C. § 12114(b).

HIPAA and ADA Protections for Housing

Part 2 does not allow for the disclosure of SUD treatment information to a landlord or housing agency without patient consent or a court order. HR 3545 would not alter those protections. HIPAA generally does not allow for the disclosure of health information to a landlord or housing agency without patient authorization or a court order. However, HIPAA would allow for the disclosure of limited types of health information to a landlord or housing agency only if it were a necessary part of the patient's treatment – such as supportive housing.

Generally, under the ADA, a landlord or agency would not be able to discriminate against an individual with a disability and would be required to provide reasonable accommodations for him or her in housing. If an individual is suffering from an SUD, the ADA protections would generally apply and prohibit such discrimination as explained in the section on Employment Protections under HIPAA, set forth above.

HIPAA Protections in Legal Proceedings

Disclosures of patient information where the covered entity is not a party are not considered part of treatment, payment, and health care operations and would not be permitted under HR 3545. The Bill as amended also dramatically increases the protections for SUD information in any criminal prosecution or civil action. Under the HR 3545, a court order or patient consent would be required before:

- Entering the information into evidence in a civil or criminal proceeding
- Forming the part of the record or taken into account in a proceeding before a Federal agency

[11] *See* EEOC Technical Assistance Manual on the ADA § 8.5.

- Being used to conduct an investigation of a plaintiff
- Being used in any application for a warrant

HIPAA also imposes specific requirements for the use or disclosure of health information in legal proceedings, including child custody and family court cases. Where a covered entity is a party to a legal proceeding, such as a plaintiff or defendant, the covered entity may use or disclose health information for purposes of the litigation as part of its health care operations.[12] Where the covered entity is not a party – such as when the patient is involved in legal action with a different party, health information may only be produced in court pursuant to an order by the court or patient authorization. Under HIPAA, health information can only be produced during discovery pursuant to a court order, patient authorization or in accordance with other privacy protections. All subpoenas for records must be accompanied by notice to the patient with opportunity to object, or proof that the litigant sought a Qualified Protective Order.[13]

HIPAA Protections Relating to Law Enforcement

Disclosures to law enforcement are not considered part of TPO, and HR 3545 would not alter the current Part 2 protections and prohibitions in place against those disclosures. In addition, the vast majority of disclosures to law enforcement under HIPAA require patient authorization, a crime, emergency, threat to public health/safety, or court involvement. Similar to Part 2, generally under HIPAA a disclosure to law enforcement requires patient authorization (in limited circumstances) or a court order. HIPAA only permits the following limited disclosures to law enforcement:

[12] 45 CFR § 164.501.
[13] 45 CFR § 164.512(e).

- By an employee of a provider about the identity of a suspect who had engaged in a criminal act against the employee. Only limited demographic and related information may be disclosed for this purpose.[14]
- To report abuse, neglect or domestic violence[15], similar to Part 2's allowance for reporting of child abuse.[16]
- Where required by law, in limited situations such as reporting gunshot wounds or other injuries.[17]
- Under a grand jury subpoena,[18] or for an administrative request, civil or investigative demand or similar process, provided the information sought is relevant and material; specific and limited in scope, and de-identified information could not reasonably be utilized.[19]
- Certain identifying information to identify or locate a suspect, fugitive, material witness or missing person.[20]
- If the patient is a victim, then after consent or in the event of an emergency, to law enforcement to assist the victim (but never to be used against the patient).[21]
- When the patient has died and the death may have been the result of criminal activity.[22]
- In the event of a crime on the premises (virtually identical to Part 2's exception for a crime on program premises).[23]

---

[14] 45 CFR § 164.502(j)(2).
[15] 45 CFR §§ 164.512(b)(1) and 164.512(c).
[16] 42 CFR § 2.12(c)(6).
[17] 45 CFR § 164.512(f)(1).
[18] 45 CFR § 164.512(f)(1).
[19] 45 CFR § 164.512(f)(1).
[20] 45 CFR § 164.512(f)(2).
[21] 45 CFR § 164.512(f)(3).
[22] 45 CFR § 164.512(f)(4).
[23] 45 CFR § 164.512(f)(5).

- In an emergency not on the premises, where the emergency medical provider needs to disclose the information to alert law enforcement of a crime.[24]
- To avert a serious threat to health or safety of the patient or others ("Duty to Warn" exception).[25]
- In limited circumstances where necessary to apprehend an individual participating in a violent crime or who has escaped from prison.[26]
- To provide healthcare to inmates and those in custody.[27]

Part 2 Limits the Sharing of SUD Treatment Information – Even Within the Same Organization

A major flaw in the current Part 2 regulations is the prohibition on re-disclosing SUD treatment information without another consent, court order, or exception under the regulations. Under the newly-created general designation process promulgated under the Final Part 2 regulations, a patient may consent to share his or her information with an intermediary, such as a health information exchange (HIE), accountable care organization (ACO), or other integrated care setting which may then share the information with all members of the integrated care model that possess a treating provider relationship with the patient.[28] However, a recipient of SUD treatment information within an HIE or ACO with a treating provider relationship would not be able to re-disclose that information to another participant in the same HIE or ACO without additional patient consent, rendering the new process unusable in practice.

[24] 45 CFR § 164.512(f)(6).
[25] 45 CFR § 164.512(j).
[26] 45 CFR §§ 164.512(j)(1), (2).
[27] 45 CFR § 164.512(k)(5). See generally, http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_for_law_enforcement_purposes/505.html.
[28] 42 CFR § 2.31(a)(4)(iii)(B).

First, the Substance Abuse and Mental Health Services Administration (SAMHSA) has issued guidance that establishes that "treating providers" in an HIE, ACO, or other integrated care setting cannot directly share SUD treatment information directly with other treating providers inside or outside the integrated setting.[29]

Under prior versions of Part 2 (pre-2017), an organization with mental health and SUD treatment facilities and clinicians could address the legal restrictions on sharing SUD information by using a qualified service organization agreement (QSOA) between the Part 2 program and the mental health department to share Part 2 information without client consent. The sharing of information would be allowed because it was considered to be for medical services provided by the mental health department to the Part 2 program, consistent with the terms of Part 2 and the QSOA provisions.

The Final Part 2 Rule changes the section addressing QSOAs to no longer allow for disclosures for medical purposes. This revision removes the ability of an organization to utilize a QSOA to efficiently share Part 2 information between a SUD department and other departments which are not covered by Part 2 but are part of the same organization. Under the existing Part 2 regulations, a program would need to obtain individual patient consent for it to share patient information within the same organization that is treating the patient for other conditions – both mental and physical.

---

[29] 82 Fed. Reg. 6052, 6081 (January 18, 2017).

Patient and Program Choice

The adoption of the HIPAA standards for TPO would not mandate that Part 2 programs disclose SUD treatment information to third parties. In fact, under HIPAA, a covered entity may impose additional and more stringent protections of health information, above and beyond what HIPAA requires. It is widely-known that HIPAA only mandates disclosures in two situations: (1) to the patient or individual who is the subject of the information and has requested access; and (2) to the Office for Civil Rights, Department of Health and Human Services (OCR) in response to an investigation or enforcement action (Note that in this latter situation, HR 3545 as amended would prohibit a disclosure to OCR as it would not be a disclosure to a covered entity). A Part 2 program would not have to disclose patient information without consent if it chose to continue to require it. As is the case today, Part 2 programs would still have the ability under law to control who receives that information and how with strict penalties still in place for non-compliance. Opponents of the Bill argue that if HR 3545 is adopted, Part 2 programs would freely share patient data without limitation and without due consideration for confidentiality. This view assumes that Part 2 programs will engage in dishonest and unethical acts with patient information and that to date, they have only acted with honesty and integrity because Part 2 prevented them from deviating. Having dealt with Part 2 programs and clinicians, I know that nothing could be further from the truth and that Part 2 providers are honest, trustworthy, and act with integrity.

HIPAA provides substantial protections for health information. The adoption of HIPAA standards relating only to disclosures to covered entities for TPO will allow for patient choice. Whether and to what extent a patient desires to share any health information, particularly SUD

treatment information, is a decision that should lie with the patient and not with the Part 2 program, the Substance Abuse and Mental Health Services Administration (SAMHSA) or the healthcare system.

Today, a patient cannot share their SUD treatment information freely in an HIE or ACO because consent and re-disclosure requirements imposed under Part 2 are too restrictive. Part 2 now contains a consent process that allows an intermediary, such as an HIE or ACO, to share information with those participants that have a treating provider relationship with the patient.[30] However, that consent process under Part 2 does not allow participants with a treating provider relationship to share the SUD treatment information with each other directly, and does not allow participants with a treating provider relationship to share SUD treatment information with another healthcare provider, such as the patient's primary care physician, if that physician is not a participant in the HIE or ACO. This artificial barrier prevents fully-integrated healthcare for patients wishing to include their SUD treatment information.

Any person, whether suffering from mental illness, diabetes, a SUD or multiple co-occurring conditions, should be able to share his or her health information with their healthcare providers, regardless of diagnosis, if they so desire. If someone does not wish to share their data, they should have a clear option to either opt-out or not opt-in to sharing that information.

Under HIPAA, a patient can request a restriction on use or disclosure of health information for TPO. The covered entity would determine whether it can and will accept the restriction and once

[30] 42 CFR § 2.31(a)(4)(iii)(B)(3).

it agrees, the information must be maintained in accordance with that restriction.[31] The covered entity does not need to accept the restriction unless the patient pays for an item or service out of pocket and requests that the provider not share information about that treatment or service with his or her health insurer, in which case the provider must not disclose it to the insurer.[32]

The ability to share the information for treatment, payment and healthcare operations under HR 3545 does not mean that Part 2 programs will be sharing SUD information without due concern for patient confidentiality. The Bill will allow for Part 2 programs and their patients to decide whether to share SUD treatment information.

Currently under Part 2, all programs, including those in integrated care settings – HIEs, ACOs and Integrated Health Homes – are required to segment out SUD treatment information from the health record to prevent its disclosure to other treating providers not in the same integrated care setting. Data segmentation is complex and expensive to implement. While some EHR providers, including Netsmart, can segment data, most EHR and HIE providers would need to modify their systems to do so. The cost of modifying all these systems would be significant – well beyond the amount estimated by SAMHSA. Even if mandated from the Federal level, we estimate that a robust system capable of supporting this type of segmented data would not be available for 7-10 more years. In the meantime, most providers and HIEs do not have the resources to modify their systems to support it.

[31] 45 CFR § 164.522.
[32] 45 CFR § 164.522(a)(1).

Breach Protections

The Bill as amended would apply the breach notification requirements of HIPAA to all Part 2 programs. The breach notification provisions will provide additional compliance and enforcement opportunities to ensure patient information is protected.

Under HIPAA, a covered entity must notify OCR if it discovers a breach of unsecured protected health information.[33] If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify OCR of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach.[34] If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify OCR of the breach within 60 days of the end of the calendar year in which the breach was discovered.[35]

Covered entities must notify individuals following the discovery of a breach. The individual notifications must be provided promptly and no later than 60 days following the discovery of a breach. The notice must include a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.[36]

[33] 45 C.F.R. § 164.408.
[34] Id.
[35] Id.
[36] Id.

These protections will be incorporated into Part 2 under the Bill as amended. The notification requirements of HIPAA already provide more protections and assurance of compliance than existing Part 2 requirements.

HIPAA Enforcement

Since the compliance date of the Privacy Rule in April 2003, the Department of Health and Human Services Office for Civil Rights (OCR) has received over 173,426 HIPAA complaints and has initiated over 871 compliance reviews.[37] OCR has resolved ninety-seven percent of these cases (168,780).[38]

OCR has investigated and resolved over 25,695 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates. Corrective actions obtained by OCR from these entities have resulted in change that is systemic and that affects all the individuals they serve. OCR has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates noncompliance by the covered entity or their business associate. To date, OCR has settled or imposed a civil money penalty in 53 cases resulting in a total dollar amount of $75,229,182.00.[39]

OCR has aggressively audited, investigated, penalized, and enforced the privacy and security requirements under HIPAA.

---

[37] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html, last accessed 5/3/18.

[38] Id.

[39] Id.

As of this writing, the author is unaware of a single substantive enforcement action taken under Part 2. Although the Final Part 2 Rule will increase enforcement opportunities, historically it has been HIPAA that has been enforced more stringently and more effectively than Part 2.

Conclusion

HR 3545 as amended will allow for the legitimate sharing of health information for specific treatment, payment, and health care operations purposes. The sharing of the information will only be with covered entities – those individuals and organizations that are bound by HIPAA and must have policies and procedures in place, training for their workforce, and agreements that protect the use or disclosure of all health information. Those entities could only re-disclose SUD information to another covered entity. The substantial protections and new rights and antidiscrimination provisions in HR 3545 as amended address the concerns raised by opponents and further the goal of effective, timely, and quality integrated care.