Published on *The National Law Review* https://natlawreview.com

HIPAA as the Standard of Care for Connecticut Common-Law Privacy Claims

Article By:

Caitlin C. Podbielski

The **Connecticut Supreme Court's recent decision in *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.***, — A.3d —, No. SC 18904, 2014 WL 5507439 (Conn., Nov. 11, 2014), **is the first published decision by a state's highest court holding that the Health Insurance Portability and Accountability Act of 1996**, 42 U.S.C. § 1320d et seq. ("HIPAA"), does not preempt common-law claims for negligence and negligent infliction of emotional distress against a health care provider. Equally significant is the Connecticut Supreme Court's holding that HIPAA's implementing regulations may provide the applicable standard of care for these tort claims when a health care provider compromises the confidentiality of a patient's medical records.

The *Byrne* decision also appears to be the first such decision issued since the enactment of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), which expanded HIPAA liability to business associates. Accordingly, HIPAA-covered entities, as well as their business associates, may now face the risk of increased exposure under common-law tort claims in addition to the fines and other remedies available under HIPAA and the HITECH Act.

Background of the *Byrne* Case

As part of its patient intake process, Avery Center provided Byrne with a copy of its privacy policy assuring patients that their protected health information would not be disclosed without the patient's authorization. Byrne also specifically instructed Avery Center not to release her medical records to the estranged father of her child. After the father filed a paternity action against Byrne, Avery Center was served with a subpoena for Byrne's medical records. Instead of seeking Byrne's authorization to disclose the records, obtaining a protective order or filing a motion to quash, Avery Center mailed a copy of the medical records to the court. As a result, Byrne allegedly suffered harassment and extortion threats after the estranged father viewed the medical records.

In her subsequent lawsuit against Avery Center, Byrne alleged that the health care provider: (1) violated its privacy policy by disclosing her protected health information without authorization; (2) negligently failed to use proper and reasonable care in protecting her medical file; (3) misrepresented that the privacy of her health information would be protected in accordance with law; and (4) engaged in conduct constituting negligent infliction of emotional distress.

The trial court dismissed Byrne's negligence claims, holding that HIPAA preempted "any action dealing with confidentiality or privacy of medical information." Byrne appealed, arguing that she was not asserting a claim for relief premised solely on a violation of HIPAA but that she was asserting common-law negligence claims, with HIPAA forming the standard of care. Avery Center countered that because there is no private right of action under HIPAA, "a plaintiff cannot use a violation of HIPAA as the standard of care for underlying claims, such as negligence."

The *Byrne* Decision

Preemption

The Connecticut Supreme Court reversed the trial court's dismissal of Byrne's tort claims, reasoning that HIPAA preempts state laws that are "contrary" to HIPAA. Citing 45 C.F.R. § 160.202, the court ruled that a state law is "contrary" to HIPAA where (1) it is impossible for a covered entity or business associate to comply with both the state and federal requirements or (2) the state law is "an obstacle to the accomplishment and execution of the full purposes and objectives" of HIPAA. The Connecticut Supreme Court reasoned that the regulatory history of HIPAA demonstrated that the statute was not intended to preempt "tort actions under state law arising out of the unauthorized release of a plaintiff's medical records."

The Connecticut Supreme Court relied on several federal and state court decisions holding that HIPAA does not preempt common-law tort claims or claims alleging violations of state privacy statutes arising from breaches of patient confidentiality. Amongst the cases cited by the *Byrne* court was the Minnesota appellate court decision in *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34 (Minn. App. 2009), which held that a state statutory cause of action for improper disclosure of medical records was not preempted by HIPAA because, although the remedies under the federal and state laws differ, compliance with the Minnesota Health Records Act (which provides for a private cause of action for the wrongful disclosure of an individual's medical records) and HIPAA both "discourage a person from wrongfully disclosing information from another person's health record."

Standard of Care

The *Byrne* court summarily concluded that, "to the extent it has become the common practice for Connecticut health care providers to follow the procedures required under HIPAA in rendering services to their patients, HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records . . . ." In reaching this sweeping conclusion, the Connecticut Supreme Court did not specify whether its reference to the HIPAA regulations was limited to the privacy standards set forth in 45 C.F.R. § 164.500 et seq. or more broadly to the security standards set forth in 45 C.F.R. § 164.302 et seq.

Impact of *Byrne* Ruling

The *Byrne* decision has important implications well beyond the rights of individuals to bring common-law tort claims for the unauthorized disclosure of medical records, given the Connecticut Supreme Court's holding that that a finder of fact may consider HIPAA to be the applicable standard of care governing the handling of a patient's medical records. Permitting HIPAA's privacy or security regulations to become the *de facto* standard of care for common-law tort claims gives plaintiffs a potentially powerful means to circumvent the lack of a private cause of action under HIPAA and therefore hold covered entities and their business associates liable in tort for alleged breaches of

patients' privacy.[1]

Indeed, an Indiana appellate court recently upheld a $1.4 million jury verdict in *Walgreen Co. v. Hinchy,*[2] where the plaintiff argued that, although HIPAA did not create a private cause of action, it still defined the standard of care for a pharmacist's duty to safeguard the confidentiality of the plaintiff's health information. The jury in *Hinchy* found that because the pharmacist's actions violated HIPAA, she had breached the standard of care and should therefore be held liable. The pharmacist's employer was also found vicariously liable because the jury found that the pharmacist had acted within the scope of her employment. *Hinchy*appears to be the first case resulting in a substantial jury verdict against a health care provider using HIPAA as the basis for the standard of care.

Plaintiff will undoubtedly rely on *Byrne*, *Hinchy* and similar decisions from courts in other states, including Delaware, Maine, North Carolina and West Virginia,[3] to pursue state law claims (including negligence, invasion of privacy and state privacy law) based on violations of HIPAA as the standard of care. Indeed, under the rationale of *Byrne*, a finding of a HIPAA violation by the Office of Civil Rights could obviate the need for a trial on liability on the state tort claims, with the case being tried solely on the issue of the amount of plaintiff's damages. As a result, there is a likelihood of an increase in the number of lawsuits asserting state tort actions following unauthorized releases or disclosures of protected health information if administrative, physical and technological safeguards, required by HIPAA and other state privacy laws, were not in place.

The *Byrne* ruling is particularly troubling given the Connecticut Supreme Court's apparent failure to recognize HIPAA's differing "required" and "addressable" administrative, physical and technical safeguards. When a safeguard set forth in 45 C.F.R. § 164.308, 164.310, 164.312, 164.314 or 164.316 is "required," covered entities and business associates *must* implement the safeguard. 45 C.F.R. § 164.306(d)(2). For example, as part of the "required" administrative safeguards, covered entities and business associates must conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered entity or business associate, and they must implement security measures sufficient to reduce risks and vulnerabilities identified in the risk assessment to a reasonable and appropriate level. 45 C.F.R. § 164.308(a)(1)(ii)(A), (B). In contrast, however, where the security standard is "addressable," covered entities or business associates must assess whether implementing the safeguard is reasonable and appropriate when analyzed with reference to the likely contribution to protecting protected health information or document why it would not be reasonable and appropriate. 45 C.F.R. § 164.306(d)(2). As part of the "addressable" technical security standards, a covered entity or business associate may "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate." 45 C.F.R. § 164.3128(e)(2)(ii). Thus, given the distinction between "required" and "addressable" safeguards under the HIPAA security standards, it is not clear whether a covered entity or business associate that does not encrypt electronic health information would fall below the *Byrne*court's HIPAA standard of care in the event that such an omission leads to the unauthorized access, disclosure or use of a patient's electronic protected health information.

Conclusion

The Connecticut Supreme Court remanded the *Byrne* case to the lower court for trial, where Byrne must prove damages to prevail on her negligence claims (a burden that many similar plaintiffs have had trouble satisfying in the absence of proof of actual identity theft). Regardless of the ultimate outcome of the case, covered entities and business associates should revisit their policies and procedures to ensure compliance with HIPAA's privacy and security standards. In so doing, covered

entities and business associates may avoid not only traditional enforcement actions and fines issued by regulators for violations of HIPAA, but also civil damages sought under tort theories premised on the HIPAA regulations to establish the requisite standard of care.

Thus, whether and to what extent HIPAA may be used to define the standard of care for common-law tort claims arising out of the unauthorized disclosure or use of protected health information will be dependent on state law. Covered entities and business associates should nevertheless recognize that their potential liability for HIPAA violations could extend beyond civil monetary penalties imposed by HHS/OCR to damages and other remedies awarded in civil lawsuits.

---

[1] Left unanswered by *Byrne* is whether other privacy and data security laws, such as the Family Educational Rights and Privacy Act or the Gramm-Leach-Bliley Act, may also be used to provide the requisite standard of care for common-law privacy claims.

[2] *Walgreen Co. v. Hinchy*, No. 49A02-1311-CT-950 (Ind. App. Ct., Nov. 14, 2014).

[3] *See*, *e.g.*, *Fanean v. Rite Aid Corp. of Delaware, Inc.*, 984 A.2d 812, 823 (Del. Super. 2009) (concluding that negligence claim could utilize HIPAA as ‘‘guidepost for determining the standard of care’’); *Bonney v. Stephens Mem. Hosp.*, 17 A.3d 123, 128 (Me. 2011) (“[a]lthough . . .HIPAA standards, like state laws and professional codes of conduct, may be admissible to establish the standard of care associated with a state tort claim, [HIPAA] itself does not authorize a private action”); *Acosta v. Byrum*, 180 N.C. App. 562, 568, 638 S.E.2d 246, 251 (N.C. 2006) (“defendant has been placed on notice that plaintiff will use HIPAA to establish the standard of care” and, therefore, “plaintiff has sufficiently pled the standard of care in her complaint”); *R.K. v. St. Mary’s Med. Ctr.*, 735 S.E.2d 715, 723 (W. Va. 2012), *cert. denied*, 133 S. Ct. 1738

may be used to supply the standard of care for other tort claims").

National Law Review, Volume IV, Number 336

Source URL:https://natlawreview.com/article/hipaa-standard-care-connecticut-common-law-privacy-claims