

If you have any questions about this Advisory, please contact:

MICHELLE DEBARGE
860.297.3702
mdebarge@wiggin.com

JODY ERDFARB
203.363.7608
jerdfarb@wiggin.com

PENNY SEAMAN
203.498.4333
pseaman@wiggin.com

MICHAEL MENAPACE
860.297.3733
mmenapace@wiggin.com

This publication is a summary of legal principles. Nothing in this article constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

The Connecticut Supreme Court Opens Door for Expanded Negligence Liability Based on HIPAA Violations

As the number of data breaches and federal and state enforcement actions for privacy and security violations reach new heights, Connecticut's highest court has added fuel to the fire in a decision that paves the way for individuals to use Health Information Portability and Accountability Act (HIPAA) violations as a basis for state negligence claims.

HIPAA does not provide a private right of action for violations. Only the federal or state government can seek sanctions, including fines, for HIPAA noncompliance. The absence of a private right of action under HIPAA has largely impeded private lawsuits that cite HIPAA violations as the basis for a negligence claim. Yet, in *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.*, 2014 WL 5507439 (Conn. Nov. 11, 2014), the Connecticut Supreme Court ruled that a plaintiff may use HIPAA to establish the standard of care in negligence cases.

Byrne was a patient of the Avery Center for Obstetrics and Gynecology, P.C. The putative father of Byrne's child served the Avery Center with a subpoena for Byrne's medical records in connection with a paternity action filed against Byrne. The Avery Center mailed a copy of Byrne's records to the court without filing a motion to quash the subpoena, appearing in court, or notifying Byrne. The putative father apparently accessed Byrne's medical records in the court file. Byrne sued the Avery Center for failure to use reasonable care in protecting

her medical information, including disclosing it in violation of HIPAA.^[1] The trial court dismissed these claims ruling that since HIPAA does not allow a private right of action, Byrne could not assert negligence claims against the Avery Center based on HIPAA noncompliance.

WHAT THE CONNECTICUT SUPREME COURT SAID

The Connecticut Supreme Court overturned the trial court's decision, ruling that HIPAA may inform the negligence standard of care in certain circumstances. The court recognized that HIPAA does not grant a private right of action, but also concluded that state causes of action are not preempted solely because they impose liability over and above that authorized by federal law. The court stated that allowing private individuals to bring negligence claims in state courts supports HIPAA's goals by establishing "another disincentive to wrongfully disclose a patient's health care record."

The court further ruled that HIPAA may be used to inform the standard of care, to the extent that HIPAA has become common practice for Connecticut health care providers. According to the court, its ruling is consistent with the general rule allowing courts to consider statutes and regulations in determining the applicable standard of care in negligence cases.

CONTINUED ON NEXT PAGE

The Connecticut Supreme Court Opens Door for Expanded Negligence Liability Based on HIPAA Violations

Importantly, the court pointed out that state court pretrial practices must be HIPAA compliant. The court referenced a 2007 Connecticut superior court case in which the court concluded that submitting medical records to a court, even if under seal, is a disclosure under HIPAA. The superior court further concluded that even if a state statute allows the disclosure of health information in response to a subpoena, a health care provider must still comply with HIPAA's more stringent provisions.

WHAT THE COURT DIDN'T SAY

Despite its noteworthy rulings, the court declined to address whether the Avery Center actually violated HIPAA, citing the undeveloped factual record. It is important to note, however, that HIPAA covered entities (and individuals acting on behalf of covered entities) may not disclose protected health information in response to a subpoena in connection with a judicial or administrative proceeding unless one of the following conditions are satisfied:

1. *The party seeking the information or covered entity demonstrates that reasonable efforts have been made to ensure that the individual who is the subject of the requested protected health information has been given notice of the request.* The party or covered entity must show that (a) it made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); (b) the notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(c) the time for the individual to raise objections to the court or administrative tribunal has elapsed, and no objections were filed or all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

2. *The party seeking the information or covered entity demonstrates that reasonable efforts have been made to secure a qualified protective order.* The party or covered entity must provide a written statement and accompanying documentation demonstrating that (a) the parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or (b) the party or covered entity has requested a qualified protective order from the court or administrative tribunal.
3. *The subpoena is accompanied by a court or administrative tribunal order that compels disclosure.*

Covered entities must also comply with HIPAA's minimum necessary standard, which requires that disclosure of protected health information be limited to only the minimum amount necessary to accomplish the intended purpose of the disclosure.

In addition, even if the HIPAA requirements are met, other federal and state laws may be applicable. For example, federal and state laws impose more restrictive standards on the disclosure of certain sensitive information, such as mental health information or certain substance

abuse treatment information. Because the laws regarding the disclosure of health information are complex, involving overlapping and even seemingly contradictory requirements, it is essential to have clear policies and procedures in place to ensure compliance. Instead of dealing with these requests on an ad hoc basis, organizations would be well-served to have a well thought out approach planned in advance.

IMPLICATIONS OF THE DECISION

Byrne has spurred much speculation that courts will now be inundated with state negligence claims alleging HIPAA violations. Some even predict that the case may lead to a proliferation of class actions based on HIPAA violations. The Connecticut Supreme Court now joins some other courts that have already similarly ruled that state-based negligence claims involving breaches of protected health information are not preempted by HIPAA. Just last year, a jury in Indiana awarded a \$1.44 million verdict against Walgreens for mishandling a customer's protected health information in a manner prohibited by HIPAA. In that case, a Walgreens pharmacist inappropriately accessed the customer's prescription record. The pharmacist then disclosed the information to her husband, with whom the customer allegedly had a relationship. The court allowed the plaintiff to use HIPAA as the standard of care to prove that Walgreens had acted negligently.

While *Byrne* may open the door to HIPAA-based negligence claims, there are other elements that must be alleged and proved in order for these claims to be successful. For example, negligence claims require proof of damages, which may be a difficult hurdle to

CONTINUED ON NEXT PAGE

The Connecticut Supreme Court Opens Door for Expanded Negligence Liability Based on HIPAA Violations

surmount in cases alleging a privacy breach depending on the factual circumstances. Moreover, the court in *Byrne* did not address the underlying question of whether Connecticut's common law provides a remedy for a health care provider's breach of its duty of confidentiality in the course of complying with a subpoena.

Although the Connecticut Supreme Court's holding permitting the use of HIPAA as the standard of care was limited to negligence actions, the court laid the groundwork for the use of HIPAA in other types of claims as well, such as claims under the Connecticut Unfair Trade Practices Act (CUTPA). For example, the court noted that the trial court relied on *Fisher v. Yale University*, No. X10NNHCV044003207S, 2006 WL 1075035 (Conn. Super. Ct. Apr. 3, 2006). The *Fisher* court ruled that HIPAA cannot be used to allege a claim under CUTPA. In overturning the trial court's decision, the court left open the question whether a HIPAA violation now may be used to support a CUTPA claim. However, a successful CUTPA claim requires the plaintiff to allege and prove different elements than those required for a negligence claim.

Insurance companies and insureds should similarly consider the impact of the *Byrne* holding as it relates to covered occurrences or intended exclusions under liability policies. Insurers and insureds will sometimes agree to exclude claims from coverage that result from alleged or actual HIPAA violations. Those exclusions should now be reviewed. For example, if the intent is to exclude only causes of action "brought pursuant to HIPAA," then the exclusion should say so expressly. But, if the intent is broader than that, and

the parties intend to exclude all causes of action that rely on HIPAA as the standard of care for negligence actions, then the insurance policy wording may need to be adjusted to exclude all claims that "relate to" or allege breaches of HIPAA standard without regard to whether the plaintiff is a government agency or a private plaintiff. Insurers and insureds would be wise to review the specific wording of their policies and any HIPAA exclusion provisions in light of *Byrne*'s distinction between causes of action brought under HIPAA and those brought as negligence actions alleging violations of the standard of care established by HIPAA.

Regardless of the scope of the potential implications of *Byrne*, those obligated to comply with HIPAA should ensure that they are fully HIPAA compliant. In particular, they should review their processes for responding to third-party subpoenas and change them as necessary to ensure compliance in the wake of the decision. Aside from the heightened risk of private lawsuits that may result from *Byrne*, HIPAA enforcement from both federal and state agencies has risen exponentially. Enforcement action is more frequent and settlement amounts are climbing ever higher. The federal government has also begun its second round of audits of HIPAA-covered entities and is expected to begin auditing business associates in 2015. Those obligated to comply with HIPAA must complete and document inventories and assessments in connection with the protected health information that they receive, access, maintain or transmit; develop and implement HIPAA-compliant policies and procedures; train workforce members; and enter into HIPAA business

associate agreements with covered entities and other subcontractors, as applicable.

Wiggin and Dana regularly counsels state, national and international clients on compliance with HIPAA and other federal privacy and security requirements. We advise clients in the development of privacy and data security policies and procedures, and help with implementation and internal auditing. We assist clients in preventing and responding to data mismanagement and data breaches, including implementing breach notification, mitigation, and corrective action strategies. We also handle litigation and state attorney general and federal investigations of alleged data breaches.

[1] Byrne also sued the Avery Center for breach of contract and negligent misrepresentation alleging that the Center violated representations in its privacy policy. The trial court did not dismiss these claims.