WIGGIN
WIGGIN AND DANA

ADVISORY

JANUARY 23, 2018

THE CONNECTICUT SUPREME COURT RECOGNIZES A NEW CAUSE OF ACTION FOR THE BREACH OF A HEALTH CARE PROVIDER'S DUTY OF CONFIDENTIALITY

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

ERIKA L. AMARANTE
203-498-4493
eamarante@wiggin.com

KEVIN S. BUDGE
203-498-4378
kbudge@wiggin.com

MICHELLE WILCOX DeBARGE
203-498-4312
mdebarge@wiggin.com

As data breaches continue to make national headlines, the stakes keep rising. In its second decision in *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.*, the Connecticut Supreme Court recognized a new negligence cause of action for a health care provider's unauthorized disclosure of confidential patient information. In doing so, Connecticut joins neighboring states, including New York and Massachusetts, which had already recognized state-law civil liability premised on the unauthorized disclosure of patient information.

THE 2014 AND 2018 CONNECTICUT SUPREME COURT DECISIONS

The defendant in *Byrne* is Avery Center for Obstetrics and Gynecology, P.C., which was served with a subpoena that instructed its record-keeper to appear at the New Haven Regional Children's Probate Court with a copy of Ms. Byrne's medical records. The subpoena was issued in a paternity action filed by Ms. Byrne's ex-boyfriend, Andro Mendoza. The Avery Center responded to the subpoena by mailing a copy of Ms. Byrne's medical records to the court. Importantly, the Avery Center admitted that it did not comply with the regulations promulgated under the federal Health Insurance Portability and Accountability Act ("HIPAA"), which permit the disclosure of medical records in response to a subpoena, but only if certain conditions are satisfied. Nor did the Avery Center file a motion to quash the subpoena, appear in court, or submit the records under seal. Mr. Mendoza accessed Ms. Byrne's medical records in the court file, and he allegedly used her health information to harass and embarrass her and her family.

HIPAA does not grant individuals the right to sue for violations—HIPAA is enforced by the Office for Civil Rights, which may levy fines and criminal penalties for violations. In the 2014 *Byrne* decision ("*Byrne I*"), however, the Connecticut Supreme Court ruled that HIPAA does not preclude state causes of action that impose liability over and above that authorized under federal law. The Court stated that the HIPAA regulations may be used to establish the standard of care in a negligence action under Connecticut law, but the justices stopped short of recognizing a negligence cause of action for a health care provider's breach of confidentiality in the course of complying with a subpoena. In its 2018 decision ("*Byrne II*"), the Court took the next step, concluding that a negligence action is recognized under Connecticut

CONTINUED

WIGGIN
WIGGIN AND DANA

NEW CAUSE OF ACTION FOR THE BREACH OF A HEALTH CARE PROVIDER'S DUTY OF CONFIDENTIALITY

law for the disclosure of confidential information obtained in the course of a physician-patient treatment relationship "unless the disclosure is otherwise allowed by law."

Byrne addressed the narrow issues of whether the Avery Center met its legal obligations when it responded to Mendoza's subpoena, and whether a non-compliant response gives rise to a civil claim for damages under Connecticut law by the patient whose records are disclosed. After the Court decided that a civil remedy exists, it considered the Avery Center's argument that it was not liable because the disclosure was made pursuant to a subpoena. The Court soundly rejected that argument. It ruled that the mere existence of a subpoena, "regardless of the method by which a health care provider chooses to comply," does not shield health care providers from liability. Providers must comply with HIPAA's regulations for responses to subpoenas—which we summarized in our 2014 advisory on *Byrne I* (please click here)—as well as applicable state law. The Court also referenced court rules pertaining to filing medical records in court, including the requirement that they be submitted in a sealed envelope, and rules regarding how medical records may be inspected. In addition to the rules specifically cited in *Byrne II*, other Connecticut court rules may come into play, including Connecticut Practice Book Rule 4-7, which requires that the filer redact certain personal-identifying information from court records in civil and family cases. Because several federal and state statutes and court rules may need to be considered when responding to a subpoena, health care providers should ensure that their policies and procedures for responding to subpoenas address all relevant legal requirements.

BYRNE'S BROADER IMPLICATIONS

Recent headlines bear out the legal and public relations ramifications of data breaches. In 2017, for example, Equifax made headlines and provoked widespread outrage when it revealed that the sensitive personal information of over 145 million American consumers was hacked. Although the Connecticut Supreme Court decision in *Byrne* expressly addresses only causes of action founded on health care providers' disclosures of patient information, plaintiffs could seek to extend the principles articulated in *Byrne* to other contexts. Therefore, all organizations and companies that maintain personal information should review their privacy policies and practices to ensure compliance with federal and state privacy requirements. They also should review their insurance policies to determine whether they have appropriate coverage for privacy violations and cyber breaches.

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.