Frustrated with Change Healthcare breach, senators propose removing limits on HIPAA fines

The current law caps fines at around $2 million per violation, which lawmakers say isn't enough

By Brittany Trang
Oct. 23, 2024
Health Tech Reporter STAT News

Linda Barbour thought she was more interested in the Change Healthcare cyberattack than most. Having worked as a medical director for several large health insurance companies and having suffered through the Change fiasco herself as a rehab doctor with a private practice in Kansas City, she figured that if her data had been exposed in that February breach, she would have been notified by now.

Barbour did finally get a letter from Change — in October. "Getting it at this point, this delayed, there's really nothing that I could do because so much time had passed," she said.

By law, companies have 60 days to notify individual customers if their personally identifiable health data was compromised. Missing that deadline could attract fines from the HHS, but it's unclear if that deadline applied to Change because it did not contract with patients directly, and because of a lack of clarity in how the Department of Health and Human Services defines when the clock starts after a breach.

In May, the CEO of Change's parent company, UnitedHealth Group, told Congress that roughly one-third of Americans' data were likely implicated in the ransomware attack. Even though the Change Healthcare cyberattack happened 8 months ago, patients are still learning for the first time that their data privacy was breached. Senate

lawmakers are aiming to change that with legislation directly aimed at the Change Healthcare fallout.

Democratic Senate leaders have introduced a bill that targets what they think is one of the root causes of why large, third-party companies like Change Healthcare can afford to blow past legal deadlines for data breaches: The fines pale in comparison to the size of the corporations that now increasingly steward Americans' health data.

In legislation introduced last month, Senators Ron Wyden (D-Ore.) and Mark Warner (D-Va.) proposed lifting the cap on fines for violations of HIPAA security practices — the federal law that established standards for protecting patients' electronic health information from disclosure without their consent. It's unlikely the bill — which is not bipartisan and doesn't have a companion bill in the House — will become law, Warner acknowledged in an interview with STAT. But this is not an issue that is going to go away, he said.

The bill sends a clear message about how Wyden, the chairman of the Senate Finance Committee, thinks cybersecurity should be regulated for the health care industry, said a committee aide.

While announcing the legislation, Wyden took aim at the Change Healthcare debacle, declaring, "Megacorporations like UnitedHealth are flunking Cybersecurity 101." The current cap on fines "prevent[s] the regulator from issuing fines large enough to deter megacorporations from ignoring cybersecurity standards," he said in a press release.

The current law caps fines at around $2 million per violation. In what was the largest U.S. health data breach at the time, insurer Anthem a few years ago paid $16 million in fines for a data breach in which the personal health information of almost 79 million people was stolen.

While hefty for a single doctor's office, as more third-parties and large corporations handle enormous amounts of sensitive patient data, those capped fines become too weak to incentivize compliance for big companies like UnitedHealth Group, a finance committee aide said. In 2023 alone, UnitedHealth Group posted $22 billion in profit. The new bill would set fines according to the size of the company and how well it tried to comply with requirements.

According to Iliana Peters, formerly a senior advisor for HIPAA compliance and enforcement at HHS' Office for Civil Rights and now an attorney at law firm Polsinelli, the main way HHS keeps health organizations in line with HIPAA law currently is via these fines.

When she was at HHS seven years ago, Peters explained, the enforcement program's goal was to fix the issues causing companies to violate HIPAA rules. "OCR's not doing that anymore. They are leaving ongoing violations at entities and fining them for those violations rather than attempting to assist the entity in fixing them," she said. The effectiveness of this form of oversight is further diluted by the fact that the fines also take a long time to materialize — Peters said that OCR often takes near the full six-year statutory limit to issue fines: For example, the Anthem breach happened in 2015, but the fines weren't handed down until 2020.

"I think that the greater penalty will be an incentive," Sen. Warner said, though he's more concerned with preventing these incidents from happening in the first place. "There will have to be some level of minimum cybersecurity standards in health care. I'd like to have it put in place before there's some major tragedy. But I can find very few people in the field that don't quietly acknowledge how we just can't continue to do this on this loose voluntary basis."

The proposed bill would also provide funding to hospitals, including rural and urban safety net hospitals, for implementing new cybersecurity minimum standards; require health care executives to undergo jail time if they lie about their compliance with cyber requirements; institute audits and stress tests for simulating recovery after a cyberattack; and introduce a user fee structure to support oversight and enforcement from HHS, much like the pharmaceutical and medical device industries are required to pay fees for the Food and Drug Administration to review their products.

Wyden in particular is still looking for answers on what happened in the Change Healthcare cyberattack. Last week, he issued another letter to UnitedHealth demanding answers to questions the senator said has asked several times without getting satisfactory answers from the company.

The reason why the data breach notifications are coming late is also complicated because Change Healthcare is not a health care provider itself, but rather a third party which processes insurance claims and helps facilitate insurance approvals and payments — making it, according to HIPAA law, a "business associate." The law says that business associates like Change have 60 days from the date the breach was discovered to tell the hospital or doctor's office that was directly connected to the patient that a breach occurred.

That health care provider is ultimately responsible for telling patients that their data has been breached. This caused much consternation earlier this year among industry groups representing health care providers because the breach wasn't a result of any of their actions and they did not want to be seen as responsible. They also did not want to be fined for not notifying their patients about the breach when UnitedHealth said it would notify providers' patients on their behalf.

It's unclear when the clock started for Change Healthcare, given the complexities of the situation, and even lawmakers are out of the loop. Sen. Warner told STAT, "We don't know whether Change is in violation of the deadline set by HIPAA," though his office would inquire with HHS.

HHS did not respond to a request for comment from STAT.

Peters, the attorney, said that in some circumstances, especially when a lot of data was stolen, it is "just impossible" to figure out whose data has been breached and get their addresses within the 60 day period. UnitedHealth CEO Andrew Witty said as much in his testimony to Congress May 1, telling senators it would take "several months" to be able to notify all impacted.

Tyler Mason, a spokesperson from UnitedHealth, told STAT in a statement that UnitedHealth is notifying impacted patients as quickly as possible and on a rolling basis, "given the volume and complexity of the data involved and the investigation is still in its final stages." He also said that UnitedHealth is in regular communication with HHS and other regulators regarding its notification process.

Physicians are scared straight about breaching private health information, whether it's during their medical training, or when they're brought on board to a hospital or payer, said Barbour, who has worked for UnitedHealth's Optum in the past. "So to see this happen in this magnitude and then to not be informed timely within the required guidelines is really concerning [...] in terms of trusting that the regulations are going to be enforced, and that companies as large as United aren't complying with them."