

August 19, 2020

First Circuit Decision Underlines Risk of Criminal HIPAA Enforcement

By: Joshua M. Robbins and Andrea R. Musker

On August 6, 2020, the U.S. Court of Appeals for the First Circuit [affirmed the conviction](#) of Massachusetts gynecologist Rita Luthra for criminal HIPAA violations and obstructing a health care investigation. Although such HIPAA prosecutions are uncommon, the case underscores the risks health care providers and others run when handling protected patient information and when speaking with government investigators.

The Luthra Prosecution

Luthra's case arose from a broader investigation of pharmaceutical company Warner Chilcott, which pled guilty to paying kickbacks to doctors under the guise of a sham "speaker series." Luthra, who received over \$23,000 from the company through the program, prescribed its osteoporosis medications to a number of her patients. According to the government indictment, when Luthra fell behind on completing prior authorization forms required for insurance coverage for the drugs, she asked a Warner Chilcott sales representative to help her medical assistant complete the forms, using confidential patient records.

As part of the larger Warner Chilcott investigation, special agents from the Health and Human Services Office of Inspector General visited Luthra's office and interviewed her. During the interview, Luthra admitted she had asked the drug rep to help with prior authorizations, but denied that he had access to protected patient information. She also gave conflicting information regarding what she had done to earn the payment from Warner Chilcott, alternately claiming it was for reviewing others' clinical research and that it was for writing a research paper.

The government charged Luthra with criminal HIPAA violations and with obstructing a health care investigation. She was convicted at trial on both counts. The First Circuit upheld the convictions, finding that there was sufficient evidence to convict as to both.

Buchalter

CLIENT ALERT

Earlier in the same investigation, a Warner Chilcott drug representative had [pleaded guilty](#) to a HIPAA violation similarly involving gaining access to patient files in order to help fill out prior authorization forms.

The HIPAA Criminal Statute

While virtually all health care providers are familiar with HIPAA, many may not realize that violations can be punished as federal crimes. The relevant statute is [42 U.S.C. § 1320d-6](#), which makes it illegal to knowingly “use or cause to be used a unique health identifier,” obtain individually identifiable health information, or disclose such information to another person. A person illegally “obtains” or “discloses” information if it is maintained by a HIPAA “covered entity” (as defined in HIPAA privacy regulations) and the person obtains or discloses it without authorization.

Authorized access and disclosure are not subject to prosecution, but must fit within one of the categories designated under HIPAA regulations. For example, a health care provider can provide patient information to another health care provider for purposes of patient treatment. Protected information can also be disclosed to “business associates” who provide services to health care providers such as billing, accounting, and management, as long as there is a proper business associate agreement (BAA) in place. Adherence to these technical requirements, however, is critical; providing patient information to pharmaceutical salespersons for insurance or marketing purposes without any BAA – as in Luthra’s case – is not a permitted exception.

Violation of § 1320d-6 can be either a misdemeanor (punishable by up to a year in prison or a \$50,000 fine), or – if committed under “false pretenses” or if done with intent to sell, transfer, or use the protected information for commercial advantage, personal gain, or malicious harm – can be a felony punishable by up to 5 or even 10 years in prison and a \$250,000 fine. Although Luthra was sentenced to probation, the First Circuit noted that the conviction “may adversely affect [her] in her professional capacity.” Indeed, such a conviction can lead to obvious reputational harm, as well as potential issues with state licensing bodies.

Buchalter

CLIENT ALERT

A Potentially Growing Trend

Although HIPAA criminal prosecutions are historically rare, there have been a number in recent years in addition to the Warner Chilcott cases. For example, in 2015, a Texas hospital employee was [sentenced](#) to 18 months in prison after pleading guilty to accessing HIPAA information with the intention of using it for personal gain. In 2016, an Ohio respiratory therapist was convicted of accessing protected information without authorization. And in 2017, Aegerion Pharmaceuticals [agreed to pay](#) over \$35 million to resolve criminal liability resulting from its sales force's multiple HIPAA violations; a Georgia pediatric cardiologist later [pled guilty](#) to illegally disclosing patient information in a related case.

Prosecutors may view HIPAA charges as useful tools in larger fraud and kickback investigations like that of Warner Chilcott. To obtain a conviction, the government does not need to prove the defendant knew his actions violated HIPAA; it must only show that he knew he was accessing the relevant information without authorization. This can be easier to explain to a jury than a more complex fraud scheme, and can provide leverage to induce lower-level figures in fraud investigations to cooperate against others. It can also provide a "fallback" charge when kickback or fraud charges are not sustainable, as in Luthra's case.

Tips for Providers

To avoid potential criminal exposure, providers should ensure they have written policies in place that direct the proper handling to patient health information, restricting access to only those persons covered by applicable HIPAA exceptions. These policies should be reviewed and updated regularly to ensure they are consistent with current regulations. They should also be complemented with regular training for all employees who handle or access patient records, accurate and thorough recordkeeping regarding of any disclosures, and adherence to the provider's notice of privacy practices. In addition, providers must have written business associate agreements in place, when appropriate, to ensure the disclosure of patient information is in compliance with the strict requirements of HIPAA and further to obligate the third-party recipients of the information to maintain the privacy and security of the information.

Just as importantly, providers should be very cautious when speaking with government investigators, whether regarding HIPAA compliance or any other issue. Inconsistencies, mistakes, or inaccurate recollections can later be used as evidence of criminal intent, or even as the basis

Buchalter

CLIENT ALERT

for separate criminal charges – such as the obstruction charge against Luthra. This risk is pronounced when discussing conduct covered by complex rules such as HIPAA and other health care regulations. A better practice is to involve experienced counsel before any interactions with law enforcement agents such as those from HHS-OIG, or any other government personnel investigating regulatory compliance.

As the First Circuit noted in Luthra’s case, “[m]odern medical practice entails endless regulation and frightening penalties.” Providers handling confidential patient information should take that warning to heart.



Joshua M. Robbins is a Shareholder and Chair of Buchalter’s White Collar and Investigations Practice in the Los Angeles and Orange County offices. He can be reached at Jrobbins@buchalter.com or 949.224.6284.



Andrea R. Musker is a member of the Health Care Practice Group Buchalter’s Los Angeles office. She can be reached at Amusker@buchalter.com or 213.891.5145

This communication is not intended to create or constitute, nor does it create or constitute, an attorney-client or any other legal relationship. No statement in this communication constitutes legal advice nor should any communication herein be construed, relied upon, or interpreted as legal advice. This communication is for general information purposes only regarding recent legal developments of interest, and is not a substitute for legal counsel on any subject matter. No reader should act or refrain from acting on the basis of any information included herein without seeking appropriate legal advice on the particular facts and circumstances affecting that reader. For more information, visit www.buchalter.com.