COSMOS
Navigate the Compliance Universe

Compliance Today - June 2024

Jonathan A. Porter (jonathan.porter@huschblackwell.com, linkedin.com/in/jonathanaporter/) is a Partner at Husch Blackwell LLP in Washington, DC.

AI can do amazing things with PHI, but be mindful of past criminal HIPAA cases

by Jonathan A. Porter

By now, everyone has seen the promises of artificial intelligence (AI) in healthcare. A program that rapidly interprets all of a patient's medical records, images, scans, and tests, and then drives the right inquiry into that patient's medical problems. That seems like a superpower to bestow upon physicians.

However, for AI to meet its full potential in healthcare, it needs access to the full panoply of protected health information (PHI). That prospect likely sends shivers down the spines of every covered entity (CE) in the United States. How can AI do its job while still securing PHI and ensuring responsible use of PHI? That is a broader topic than what this author is prepared for.

Instead, this article sets the outer limits of PHI misuse: criminal prosecutions for HIPAA violations. Recognizing the facts that gave rise to criminal convictions for abusing patient privacy is useful in that it gives a name to the things to be avoided at all costs in implementing AI and other useful technologies promising to revolutionize healthcare in America. In addition, we will examine the basics of criminal HIPAA violations and some of the rare previous cases against individuals accused of violating HIPAA in a criminal fashion.

42 U.S.C. § 1320d–6, in a nutshell

The criminal arm of HIPAA is found in 42 U.S.C. § 1320d–6. In essence, the law prohibits CEs from knowingly violating HIPAA by obtaining or disclosing individually identifiable health information without authorization. The term "individually identifiable health information" is broad, applying to anything created or received by a CE that both relates to some aspect of a patient's healthcare and identifies a particular patient (or can be reasonably used to do so).[1] Thus, virtually every patient-related record in a CE's practice could give rise to HIPAA violations under the definition.

The consequences of violating 42 U.S.C. § 1320d–6 depend on the violator's motive. Those who violate the statute with the intent to "sell, transfer, or use" PHI for "commercial advantage, personal gain, or malicious harm" are subjected to the most serious consequence under the statute: imprisonment for up to 10 years.[2] The absence of commercial advantage still results in a serious consequence, so long as the violation is committed under false pretenses, with that violation resulting in imprisonment for up to five years.[3] But if a CE violates HIPAA in a way that results in no commercial advantage, personal gain, or malicious harm, and is not committed under false pretenses, then that CE is subjected to a misdemeanor: imprisonment for not more than one year.[4]

What conduct results in criminal HIPAA prosecutions?

While the statute is broad in reach, criminal HIPAA prosecutions are in reality relatively rare. Often, the most egregious schemes that violate HIPAA are typically wrapped into various fraud charges, which carry even heavier penalties and treatment under the U.S. Sentencing Guidelines. Similarly, people who obtain PHI intending to steal a patient's identity in some ways are typically prosecuted under identity theft statutes. However, those identity thieves can still be prosecuted under HIPAA. One example is the very first criminal HIPAA prosecution in the case of *United States v. Richard Gibson*.[5] In that case, the defendant was a technician at a Seattle, Washington-based cancer center. Gibson was convicted of using a patient's identity—learned from the cancer center's files—to acquire credit cards in the patient's name, incurring over $9,000 in fraudulent charges.

But prosecutions for nonfraudulent, nonidentity theft HIPAA violations are relatively rare. Yet, we can learn a lot from those rare types of HIPAA cases, which can be boiled down to two types: malicious acts and giving PHI access to sales reps.

Malicious HIPAA violations

One clear category of criminal HIPAA prosecutions is where individuals weaponize health information for malicious purposes. The best example of this type of prosecution is the case of *United States v. Linda Sue Kalina*.[6] Kalina was a patient information coordinator with affiliated medical centers and thus had access to a range of PHI.[7] Using that special access, Kalina was accused of, and ultimately pled guilty to, viewing PHI of individuals for personal, nonmedical reasons.[8] The investigation revealed that Kalina accessed PHI of 111 patients, including—according to the press release announcing Kalina's sentence of imprisonment—"coworkers, former classmates, and relatives."[9]

However, that access did not result in Kalina's criminal prosecution. The triggering event was when Kalina then disclosed two individuals' PHI relating to their "personal gynecological health information . . . with the intent to cause those individuals embarrassment and mental distress," according to the U.S. Department of Justice's (DOJ) press releases announcing Kalina's guilty plea and sentence.[10]

The judge overseeing Kalina's case sentenced her to the top end of the advisory guidelines range for the offense: one year imprisonment.[11] According to the DOJ press release announcing the sentence, the federal judge labeled Kalina's conduct as "the most egregious of its kind."[12]

Giving access to sales reps

In the modern practice of medicine, sales reps often become integrated with a medical practice, making it easy to cross a line when it comes to patient privacy, as many individuals have discovered.

One recent example is the case of *United States v. Frank Alario*,[13] a former physician who pled guilty to a criminal HIPAA charge.[14] Alario allowed a pharmaceutical sales representative to access his office, his medical files, and patient information as part of a plan for the sales representative to generate prescriptions for compound medications. Alario not only allowed the sales representative to access patient files, but he also brought the sales representative into patient exam rooms, causing patients to believe that the sales representative was part of Alario's medical staff.[15] The sales representative then would generate prescriptions using the information learned from Alario's patient files and exams, which Alario would then sign.[16]

The pharmaceutical sales representative also pled guilty as part of the scheme, including the sales representative receiving kickbacks from a Louisiana compounding pharmacy receiving the Alario compound prescriptions.[17]

However, DOJ did not allege that Alario himself was receiving kickbacks. Instead, Alario pled guilty only to a criminal HIPAA violation, for which he was sentenced in July of 2023 to one year of probation but no prison time.[18]

The lesson from Alario's prosecution is to keep proper barriers between healthcare providers and individuals with whom the providers do not have adequate HIPAA-compliant agreements and patient authorizations.

Another example involving inappropriate barriers between physician staff and sales representatives is the case of *United States v. Rita Luthra*.[19] Luthra was a physician whom a pharmaceutical company paid to speak about particular drugs and who also commonly prescribed those particular drugs to her patients.[20] The wrinkle was that these particular drugs were typically not covered by patients' prescription drug plans because a less expensive generic drug was available, and so additional documentation explaining why each patient needed the name brand drug as opposed to generic was required by Luthra for the particular drugs to be covered.[21]

The volume of prescriptions apparently became significant, as did the paperwork required of Luthra to ensure coverage for these drugs. Luthra allegedly asked a pharmaceutical company sales representative to assist Luthra's medical assistant in completing all the additional paperwork. This task required the sales representative to review Luthra's patient files to identify particularized grounds for prescribing the name-brand drugs over generics.[22] That is where Luthra crossed a HIPAA line, leading to her indictment.

Luthra went to trial, where her former medical assistant testified that Luthra knew that the task with which the sales representative was helping involved reviewing patient records and that Luthra actually called the medical assistant after federal agents arrived to interview personnel in Luthra's office and instructed the medical assistant to lie about whether the sales representative ever viewed patient records. A federal jury convicted Luthra of one count of aiding and abetting a HIPAA violation and one count of obstructing a criminal investigation of a healthcare offense.[23] Luthra's convictions were unsuccessfully appealed after the federal judge sentenced her to one year of probation but no prison time.

The lesson of Luthra's prosecution—besides the obvious lesson of not instructing others to lie to federal agents—is that boundaries must be respected when it comes to PHI, like with Alario's prosecution.

The more egregious version of this category is actually selling patient information like a series of defendants were accused of in a 2023 indictment in the Western District of Tennessee. In that case, hospital employees pled guilty to selling the names and phone numbers of car crash victims to an individual who then sold that patient information to personal injury lawyers and chiropractors.[24]

What can CEs learn from HIPAA prosecutions when implementing AI?

There are more unknowns than knowns when it comes to AI right now. Earlier this year, the U.S. Department of State commissioned a report on AI that concluded that AI has the potential to "pose an extinction-level threat to the human species."[25] The report identified two significant causes for concern: one, AI can respond to commands in such a way that would allow AI to essentially be weaponized; and two, that developers could lose control of AI, leading AI to generate its own commands that exceed boundaries we believe are currently in place. Other reports have sounded an alarm on AI's propensity to suscept to bias, which has its own profound concerns when it comes to healthcare.[26]

This author is ill-equipped to tackle those societal-level concerns; however, healthcare providers should take all due precautions in implementing any generative AI into their processes. Given AI's potential to be weaponized,

the next Linda Sue Kalina—who released personal gynecological information about two women for malicious purposes—could achieve much greater and wide-scale damage with the right access to PHI.

Even more concerning—given AI's potential to generate itself past barriers we think exist—great care should be taken to isolate systems to prevent AI from crossing barriers in the name of what it believes to be helpful actions to patients.

These precautions should be taken because, at the end of the day, courts will not be prosecuting computer codes for HIPAA violations but rather the humans who make the mistakes.

Takeaways

- Artificial intelligence (AI) can revolutionize healthcare, but access to large amounts of data—including protected health information (PHI)—is needed to achieve that revolution.
- At its worst, AI has the potential to get those healthcare entities implementing AI into criminal HIPAA prosecutions.
- Criminal HIPAA prosecutions have, in the past, been rare.
- Criminal HIPAA prosecutions have been brought when individuals use PHI for malicious reasons and when they grant sales representatives improper access to PHI.
- Given concerns that AI can be weaponized and generate its own commands to exceed what we believe to be boundaries, those implementing AI into health systems should take great care. Otherwise, they may cause the types of HIPAA violations that result in criminal prosecution.

1 42 U.S.C. § 1320d–6.
2 42 U.S.C. § 1320d–6(b)(3).
3 42 U.S.C. § 1320d–6(b)(2).
4 42 U.S.C. § 1320d–6(b)(1).
5 United States v. Richard Gibson, Case No. 2:04-cr-374, (W.D. Wash. Aug. 18, 2004), ECF No. 4.
6 United States v. Linda Sue Kalina, Case No. 2:18-cr-175-AJS, Doc. 1 (Indictment) (W.D. Pa. June 28, 2018); U.S. Department of Justice, U.S. Attorney's Office for the Western District of Pennsylvania, "Butler Woman to Serve a Year in Prison for Maliciously Disclosing Personally Identifiable Health Information," news release, June 25, 2019, https://www.justice.gov/usao-wdpa/pr/butler-woman-serve-year-prison-maliciously-disclosing-personally-identifiable-health.
7 Case No. 2:18-cr-175-AJS, Doc. 1 (Indictment) (W.D. Pa. June 28, 2018), 5.
8 Case No. 2:18-cr-175-AJS, Doc. 33-1 (Plea Agreement) (W.D. Pa. Mar. 6, 2019).
9 U.S. Department of Justice, U.S. Attorney's Office for the Western District of Pennsylvania, "Butler Woman to Serve a Year in Prison for Maliciously Disclosing Personally Identifiable Health Information."
10 U.S. Department of Justice, U.S. Attorney's Office for the Western District of Pennsylvania, "Butler Woman to Serve a Year in Prison for Maliciously Disclosing Personally Identifiable Health Information"; U.S. Department of Justice, U.S. Attorney's Office for the Western District of Pennsylvania, "Former Patient Coordinator Pleads Guilty to Wrongfully Disclosing Health Information to Cause Harm," news release, March 6, 2019, https://www.justice.gov/usao-wdpa/pr/former-patient-coordinator-pleads-guilty-wrongfully-disclosing-health-information-cause.
11 U.S. Department of Justice, U.S. Attorney's Office for the Western District of Pennsylvania, "Butler Woman to Serve a Year in Prison for Maliciously Disclosing Personally Identifiable Health Information."

12 U.S. Department of Justice, U.S. Attorney's Office for the Western District of Pennsylvania, "Butler Woman to Serve a Year in Prison for Maliciously Disclosing Personally Identifiable Health Information."
13 United States v. Frank Alario, Case No. 20-cr-764-2 (RBK), Doc. 1 (D. N.J. Sept. 9, 2020).
14 United States v. Frank Alario, Case No. 1:20-cr-764 (RBK), Doc. 69 (D. N.J. Oct. 6, 2022); U.S. Department of Justice, U.S. Attorney's Office for the District of New Jersey, "Doctor Admits Criminal HIPAA Scheme for Wrongful Disclosure of Protected Patient Health Information to Pharmaceutical Sales Representative," news release, October 7, 2022, https://www.justice.gov/usao-nj/pr/doctor-admits-criminal-hipaa-scheme-wrongful-disclosure-protected-patient-health.
15 U.S. Department of Justice, U.S. Attorney's Office for the District of New Jersey, "Doctor Admits Criminal HIPAA Scheme for Wrongful Disclosure of Protected Patient Health Information to Pharmaceutical Sales Representative."
16 U.S. Department of Justice, U.S. Attorney's Office for the District of New Jersey, "Doctor Admits Criminal HIPAA Scheme for Wrongful Disclosure of Protected Patient Health Information to Pharmaceutical Sales Representative."
17 United States v. Ritson, Case No. 20-cr-764-1 (RBK), Doc. 78 (Plea Agreement) (D. N.J. Oct. 19, 2022).
18 Case No. 20-cr-764-2 (RBK), Doc. 91 (Judgment) (D. N.J. July 10, 2023).
19 Case No. 3:15-cr-30032-MGM, Doc. 3 (Indictment) (D. Mass. Oct. 21, 2015); U.S. Department of Justice, U.S. Attorney's Office for the District of Massachusetts, "Springfield Doctor Convicted by Jury of Illegally Sharing Patient Medical Files," news release, April 30, 2018, https://www.justice.gov/usao-ma/pr/springfield-doctor-convicted-jury-illegally-sharing-patient-medical-files.
20 Case No. 3:15-cr-30032-MGM, Doc. 3 (Indictment) (D. Mass. Oct. 21, 2015), 11–13.
21 Case No. 3:15-cr-30032-MGM, Doc. 3 (Indictment) (D. Mass. Oct. 21, 2015), 18, 19.
22 Case No. 3:15-cr-30032-MGM, Doc. 3 (Indictment) (D. Mass. Oct. 21, 2015), 18, 19.
23 U.S. Department of Justice, U.S. Attorney's Office for the District of Massachusetts, "Springfield Doctor Convicted by Jury of Illegally Sharing Patient Medical Files."
24 U.S. Department of Justice, U.S. Attorney's Office for the Western District of Tennessee, "Former Methodist Hospital Employees Plead Guilty to HIPAA Violations," news release, April 25, 2023, https://www.justice.gov/usao-wdtn/pr/former-methodist-hospital-employees-plead-guilty-hipaa-violations.
25 Matt Egan, "AI could pose 'extinction-level' threat to humans and the US must intervene, State Dept.-commissioned report warns," CNN, March 12, 2024, https://www.cnn.com/2024/03/12/business/artificial-intelligence-ai-report-extinction/index.html.
26 Zachary Small, "Black Artists Say A.I. Shows Bias, With Algorithms Erasing Their History," *The New York Times*, July 4, 2023, https://www.nytimes.com/2023/07/04/arts/design/black-artists-bias-ai.html.