THOUGHT LEADERSHIP FORUM

Cybersecurity/AI Forum:

Greenberg Traurig

Does the increasing ability for de-identified data to be re-identified through the use of AI-driven technology meaningfully change the risk profile (e.g., breaches) that health care companies will ascribe to certain business operations?

Potentially, yes.

There are two methods of de-identification that remove the remaining data from scope of regulation under HIPAA. In short, one method, the "Expert Determination," involves statistical analysis of the data in order to determine that it is not identifiable. The second method requires the removal of 18 identifiers. Following either of these processes, the regulator (Office for Civil Rights) considers the data de-identified and no longer regulated by HIPAA. For regulated entities, de-identified data is valuable for many purposes, including clinical research and population health assessment projection. However, to bad actors, identifiable data is typically much more valuable and worth the effort to re-identify.

De-identified data sets usually are massive and include the data of large numbers of individuals – intuitively, large data sets are more useful to identify trends. The concern here is largely regarding the ability of bad actors to match "de-identified data" with data from sources across the web (including previously stolen data sets) in order to identify the individuals listed in the de-identified data set. This calls into question whether current de-identification processes are sufficient.

In light of the increased savviness of bad actors, health care organizations may find that use and disclosure of de-identified data, even for legitimate purposes (e.g., research) is too risky, and may limit or cease the operations that rely on such data. Further, many organizations engage third-party vendors to de-identify data (rather than undertaking de-identification internally), in which case a source of risk may be the vendor itself. Thoughtful vetting of such vendors is crucial to ensure that de-identification processes are being followed, and that subsequent data is used and disclosed only as contemplated by the customer.

> **"However, to bad actors, identifiable data is typically much more valuable and worth the effort to re-identify. "**
>
> **BRAD M. ROSTOLSKY & CATHERINE E. GALEA**
> Greenberg Traurig

Do existing privacy regulations address the extent to which patients/consumers must be told that their information is being used to smarten AI tools used in the health care industry?

It depends on whom you ask.

Through HIPAA, state-level privacy laws, and Federal Trade Commission regulations, patients and consumers are currently presented (at various levels of detail) with how organizations use and disclose their health information.

Arguments can be made that existing legal regimes are timeless and apply to previously unforeseen data uses (e.g., making AI smarter), as many privacy laws already direct regulated organizations to inform individuals of data uses generally. These same laws typically require affirmative consent to particular uses, like for sale, marketing, and disclosures to certain types of third parties. Oftentimes, organizations that use health information for educating AI tools characterize such uses as part of the organization's general administrative operations and in support of the provision of existing services.

Conversely, given that many privacy-law drafters may have been unaware of the trajectory of technology, arguments can also be made that using personal health information to make AI tools smarter is

BRAD M. ROSTOLSKY
Shareholder
Greenberg Traurig

Brad is a member of the Health Care & FDA Practice in Greenberg Traurig's Philadelphia office. As a health care regulatory and transactional attorney, Brad represents a range of clients in the health sector including hospitals, health plans, medical practices, pharmacies, long term care facilities, electronic health records providers, management companies, pharmaceutical manufacturers, and medical device companies, among others. He regularly advises clients on virtually all aspects of health information privacy and security compliance under HIPAA and state law, and spends considerable time helping clients navigate the multi-specialty realm of digital health, including providing business structuring advice to facilitate pursuing desired operational outcomes without running afoul of regulatory constraints. Brad also has deep experience guiding clients through significant privacy and security incident response and associated investigations.

Brad's experience also includes assisting hospitals on arrangements with physicians, such as joint ventures, physician recruitment, practice acquisitions, and employment arrangements, as well as compliance with federal and state laws governing referrals among health care providers, such as the Anti-Kickback Statute and the Stark Law. Brad also advises clients in a variety of areas including the corporate practice of medicine, facility licensing, hospital/medical staff relationships, informed consent, and regulatory compliance in the operation of Medicare, Medicaid and other third-party reimbursement programs.

CATHERINE E. GALEA
Of Counsel
Greenberg Traurig

Catherine E. David (Galea) is a member of the Health Care & FDA Practice in Greenberg Traurig's Philadelphia office. She focuses her practice on health care regulatory, compliance, transactional, and enforcement matters. Cate concentrates her practice on the laws that govern health data, including, HIPAA, interoperability and information blocking regulations, Part 2, and similar state laws. Cate regularly handles responses to government investigations, policy drafting and implementation, and negotiating business associate agreements. She advises clients on health care licensing issues with mergers and acquisitions, fraud and abuse compliance under Stark Law and the Federal Anti-Kickback Statute, and health information privacy and security compliance under HIPAA and state law.

a use and disclosure that should require affirmative consent. Despite the lack of a directive to inform individuals of their data being used to educate AI tools in some cases, many organizations are unilaterally notifying their customers through updated terms of service and click-through consents. Many states have developed advisory councils to evaluate how best to harness AI while continuing to protect individual privacy.

Although some maintain that no additional legislation is needed to direct organizations to inform individuals of data usage for "smartening" AI, it would be unsurprising to see continued legislation addressing this issue.

In light of the manner in which AI models are trained to get "smarter," how do we best address the degree to which incomplete, inaccurate, and inconsistent data is common in the health care industry?

Data entry, in particular in the health care industry, is a human process; patients can directly input information in applications, or providers can manually add information to a patient's record. In both cases, the chances for error or omission are plentiful. Any small or large error or omission is amplified as patient data is moved through the health care system to facilitate care, payment, or other uses.

Given that AI is only as smart as the data provided for analysis, there are some concerns that health care data's historical spottiness may lead AI tools to be equally rickety. Providers should continue to focus on accurate and complete data input, while back-office operations should be mindful to develop data clean-up and minimization initiatives. Patients should also remain vigilant in ensuring their medical records reflect accurate information by critically reviewing data contained in portals, discharge summaries, and in-person visit confirmations of information.

In light of the combination of fledgling AI tools and varying levels of completeness with respect to health care data, reliance on AI-generated information must be supplemented with human evaluation. If these tools are used to amplify – and not used in place of – independent medical judgment, great strides can be made in the medical field.

Will a greater use of AI impact, one way or the other, the manner in which health care companies are impacted by ransomware attacks?

The increased adoption of AI in the health care industry has the potential to lead to both positive and negative consequences relative to how health care companies are impacted by ransomware attacks. On the positive front, AI can play a pivotal role in early threat detection by scrutinizing anomalies in network traffic and user behavior in order to expedite the response and containment processes. Furthermore, AI's capacity for predictive analytics may be able to help health care companies proactively identify system intrusion. Additionally, AI-infused capabilities likely provide an opportunity to enhance the mechanics of incident response and expedite recovery and data restoration efforts.

"As AI-based systems become more central in health care operations, they may become prime targets for ransomware attacks."

BRAD M. ROSTOLSKY & CATHERINE E. GALEA
Greenberg Traurig

As with many advancements in technology, there are likely some negative implications associated with AI, as well. AI is the very type of technology cybercriminals look to attack. As AI-based systems become more central in health care operations, they may become prime targets for ransomware attacks. Such incursions could impact patient care, diagnostics, and treatment planning. Moreover, AI systems may harbor vulnerabilities that malicious actors could exploit, posing a threat to critical operations, especially if health care institutions heavily rely on AI-driven decision-making processes. Lastly, it will be important to avoid an over-dependence on AI-driven security measures to the extent they potentially overshadow other vital security practices.

The integration of AI in health care cybersecurity necessitates a comprehensive and holistic approach. While AI has the potential to enhance security measures, it should be viewed as an integral component within a broader security framework, alongside other critical traditional security measures, to effectively manage and mitigate the impact of ransomware attacks within the health care sector.

Will the advent of machine-learning tools in the health care industry likely lead regulators to draft regulations, or can existing regulations address the use of this new technology?

While the existing health care compliance framework remains a solid foundation on which to base a strong health care regulatory compliance program, the unique challenges presented by machine learning in the health care industry have already triggered discussions for new or amended rules in the privacy space, as well as within the FDA.

The complexities associated with machine learning can make its decision-making processes opaque, raising transparency concerns. This could lead to a call for specific regulations in order to best protect patient safety and ensure equitable treatment, especially to the extent that machine-learning models make recommendations regarding treatment decisions.

Further, before even considering the extent to which machine learning will impact the health care privacy and security regulatory landscape, it is important to consider the degree to which the quality of stored data will impact the utility of health care decision making tools. Health care data is often incomplete and inconsistent. In order for machine learning tools to effectively amplify treatment capabilities, facilitate payor coverage determinations, or assist in determining an individual's cost for health care insurance, consideration should be given to the quality of the data fed into the machine-learning tool. Given this baseline concern with data input, regulators may focus on data cleaning and preprocessing activities.

Outside of the machine-learning context, we often encounter situations where certain HIPAA privacy provisions seem anachronistic, i.e., where the typical business process was not conceived of when the regulations were promulgated. The technological advances in health care that center around machine-learning capabilities present similar challenges to regulated entities and regulators alike. Both HIPAA and the 21st Century Cures Act provide broad protections to patients, as well as proscriptive rules of the road for providers, payors, and other players in the health care industry relative to how patient data can and cannot be used. Business Associate Agreement requirements under HIPAA, as well as the need for HIPAA authorizations, remain unchanged. That said, the infusion of new AI technologies and machine-learning tools will force the various regulated entities to determine the extent to which they are pushing existing regulatory boundaries. At a minimum, it seems clear that the very use of the terms "machine learning" and "artificial intelligence" in the context of health care causes uneasiness and uncertainty in some quarters.