

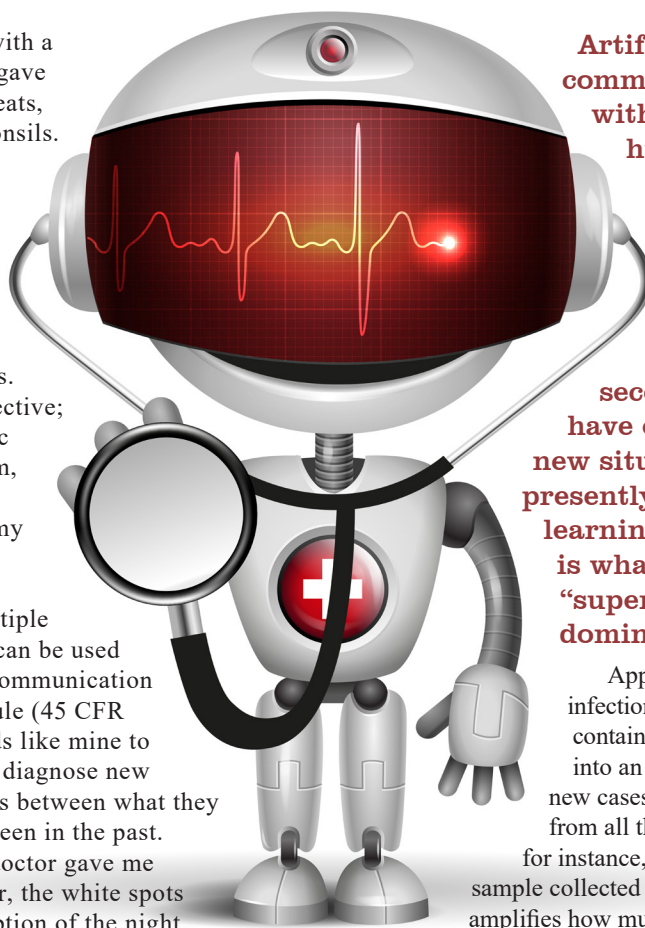
DR. BOT and Your Sacred Body

BY NICHOLAS SHOOK, ESQ.

Personally, I just dealt with a terrible throat infection that gave me a terrible fever, night sweats, trouble eating and swollen tonsils. I sought medical care from multiple facilities and was administered multiple tests, but everything came back negative. In response, my urgent care doctor gave me a wide range of antibiotics to treat a plethora of ailments. These antibiotics proved effective; however, they wreaked havoc on my gastrointestinal system, during and for a week after treatment. This hasn't been my best month.

Records of my ailment are now scattered across multiple medical offices, where they can be used in the provider-to-provider communication under the HIPAA Privacy Rule (45 CFR 164.506). Doctors use records like mine to study and learn from as they diagnose new patients, drawing correlations between what they see today and what they've seen in the past. In my case, my urgent care doctor gave me antibiotics based on my fever, the white spots on my tonsils and my description of the night sweats I was experiencing. I trusted that he made this judgment based on his prior experience with similar cases and his studies, gleaned and synthesized from other doctors' handling of their own cases.

Passing down knowledge from one generation to the next is nothing new, and it highlights scientific and academic progression for our species. For quite some time the next horizon is the use of computers to simulate how we learn and how to, in turn, accelerate our collective progress.



Artificial intelligence (AI), as commonly practiced today, deals with inputs and outputs. For humans, inputs are the foundation of what we've learned, and our outputs are how we adapt to the present. In the practice of law, we have inputs: case law, statutes and secondary authority; and we have outputs: new pleadings for new situations founded on what's presently available. Thinking of learning as inputs and outputs is what's formally known as "supervised learning," and it dominates the field today.¹

Applying supervised learning to my bacterial infection, saliva samples verified by doctors as containing some infection (or not) can be input into an AI system in order to train it to handle new cases like mine. This AI system can learn from all the saliva samples from a given provider, for instance, every single Kaiser Permanente saliva sample collected and tested for bacteria. AI significantly amplifies how much information can be used in the calculation of a new decision. Imagine if one doctor saw every tonsil in the world and knew everything about tonsils because of it. This outcome is what AI can achieve in every facet of our lives. Pretty astounding and, for those concerned about privacy, may cause big concern.

Who gets to access this holy grail of data? Most patients probably feel comfortable with their doctors and nurses having access to their medical information, but how about their billing assistants, the IT staff at a hospital or the staff at the company writing the computer software? What could the damages be if someone unauthorized gained access to your data? Stalking? Harassment? Worse? These legal questions surrounding privacy are somewhat addressed by HIPAA and will need further clarification from regulators.

continued on page 22

Dr. Bot and Your Sacred Body

Currently, HIPAA protects patient privacy by allowing an individual to choose the third party to which their information is disclosed. This person must be identified in writing by the patient with signed written consent.² However, information may be transmitted between a patient's current provider and covered entities, except for psychotherapy notes or substance abuse records.³ A covered entity is broadly defined to include health plans, health care clearinghouses and health care providers,⁴ such as all of Kaiser Permanente from the above example. Regulators have put the onus on all covered entities to protect patient confidentiality and treat all information within as a walled garden, inclusive of the vendors they choose.

Earlier this year, Aetna reached a \$17 million settlement for sending medication information to HIV patients in clear envelopes. They had used a third party vendor to stuff mailers and had lacked the oversight to see that confidential information could be plainly read through the clear envelopes.⁵

The recent Aetna/HIV mailer breach is one of many examples of providers held liable for actions taken by their vendors and sets a strict precedent for providers wishing to contract with AI vendors to improve patient outcomes.⁶ To ensure vendors are also liable, providers and vendors agree to a business associate agreement (BAA), which holds the vendor accountable for any wanton privacy breach or other violation of HIPAA.⁷ These protections ensure the vendor is accountable for all of its agents, including its employees and their own contractors, and they are self-insured against their own risk, such as in the case of a cybersecurity incident.

Under current HIPAA laws, an AI vendor like Alphabet's Verily Life Sciences can sign a BAA with a provider, such as Medicare, which allows them to use that provider's data to train their AI systems, in turn, to help that provider's future patients with their cases. With current precedent, the protections and obligations

of an AI vendor are akin to an Electronic Health Record (EHR) vendor, and the provider must be well-aware of the risks associated with unprivileged access to a treasure trove of health data. AI has already begun treating patients and assessing outcomes within the boundaries of HIPAA and other healthcare regulations. If those writing the algorithms or supervising the learning of these new systems should do something illegal with patient information, they will suffer heavy fiscal consequences in civil litigation.

Aside from unauthorized persons accessing patient data, could a patient sue the AI itself for an improper diagnosis? Probably not anytime soon; it is unlikely that we will see AI diagnosing and treating cases without a human provider present; or, in technical terms, it is unlikely we will see unsupervised AI dictating our healthcare anytime soon. Unsupervised healthcare AI could, under current laws, be interpreted as a non-provider practicing medicine, which is illegal under HIPAA. Though when that day finally comes, this article will be woefully out-of-date.

In sum, supervised AI today presents the same challenges and liabilities as any other software vendor in the healthcare space. There are risks related to who gets to see your data, but ultimately, as legal practitioners, current law equates AI to medical equipment or EHR providers: tools that assist current providers with their cases. The possibilities of AI, however, are endless. Having an AI created, all-knowing Dr. Bot look at my throat might have been comforting, because I would then have received a much more precise treatment, possibly without the side-effects, and my digestive system would have rejoiced. **NL**

1. Andrew Ng - The State of Artificial Intelligence. https://www.youtube.com/watch?v=NKpuX_yzdYs.
2. <https://www.hhs.gov/hipaa/for-professionals/faq/2036/can-an-individual-through-the-hipaa-right/index.html>.
3. [https://www.aap.org/en-us/advocacy-and-policy/aap-health-initiatives/](https://www.aap.org/en-us/advocacy-and-policy/aap-health-initiatives/Mental-Health/Pages/HIPAA-Privacy-Rule-and-Provider-to-Provider-Communication.aspx)

[Mental-Health/Pages/HIPAA-Privacy-Rule-and-Provider-to-Provider-Communication.aspx](https://www.aap.org/en-us/advocacy-and-policy/aap-health-initiatives/Mental-Health/Pages/HIPAA-Privacy-Rule-and-Provider-to-Provider-Communication.aspx).

4. https://privacyruleandresearch.nih.gov/pr_06.asp.
5. <https://healthitsecurity.com/news/17m-settlement-agreement-reached-in-aetna-data-breach-case>.
6. HIPAA Cyber Security: Your Vendor is a Back Door to Your Server https://www.healthlawyers.org/Events/Programs/Materials/Documents/FC14/I_kelly.pdf.
7. Afitble BAA <https://www.aptible.com/resources/what-is-a-hipaa-baa/#what-or-who-is-a-business-associate>.

Howard & Howard
law for business®



Mergers & Acquisitions



Commercial Litigation



Intellectual Property



Bruce Donn Cassity

BCassity@howardandhoward.com
(702) 667-4811

WE ARE PLEASED TO ANNOUNCE: Bruce Donn Cassity has joined the firm

Mr. Cassity concentrates his practice in commercial litigation, intellectual property, and real estate. Representing clients in a broad range of industries, he is passionate about his work and being involved in the community.

NICHOLAS SHOOK

is a senior software developer for Verify Investor, the leading investor platform for SEC Reg D crowdfunding compliance, and he maintains a limited practice focused on blockchain, cannabis, cybersecurity and helping friends. He can be reached by email at nick@1337lawyers.com.



www.howardandhoward.com 702.257.1483

Las Vegas, NV | Los Angeles, CA | Ann Arbor, MI | Chicago, IL | Detroit, MI | Peoria, IL