PROGRAM MATERIALS
Program #36133
April 16, 2026

# Who is Your Lawyer or Doctor - It's Not GenAI



Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

# Who is Your Lawyer or Doctor – It's Not GenAI.

Rachel V. Rose, JD, MBA

Celesq

April 2026

# Disclaimer

The information is not meant to constitute legal advice and is current as the of the date of the initial presentation. Participants are encouraged to continually review updated case law, government website, State Bar websites and other reputable and relevant sources.

# Overview

Presentation

**Overview**

**Recent Regulations, Opinions and Pending Cases**

**Terms and Conditions Highlights**

**Strategies for Combatting Risk**

**Conclusion & Questions**

# Overview

Definitions & Scenarios

# NIST DEFINITION(S) of Artificial Intelligence

- “A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self improvement.”
- ”The capability of a device to perform functions that are normally associated with human intelligence such as reasoning, learning, and self-improvement.”

*See American National Standard Dictionary of Information Technology (ANSDIT) - ANSI INCITS 172-220 (R2007).*

# Large Language Models (LLM)s

- According to Lenovo,

  “LLMs are AI systems trained on extensive datasets to process and generate human-like text. They rely on deep learning techniques, particularly neural networks, to analyze patterns in language and predict the next work or phrase in a sequence. These models are ‘large’ because they contain billions of parameters, which are the adjustable weights within the neural network that allow the model to make predictions.”

# NIST DEFINITION OF ALGORITHM

A clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result.

- Sources: NIST SP 800-107 Rev.

# What is Data Scraping?

- Data scraping, which may be legal or illegal, is the process of utilizing software to extract swaths of valuable data, usually from a website or across multiple websites.

# ISO Definition – Generative AI

"[G]enerative AI, which differs from traditional AI in its capabilities and application. **While traditional AI systems are primarily used to analyse data and make predictions, generative AI goes a step further by creating new data similar to its training data.**"

www.iso.org

# Evaluation of Large Language Model Chatbot Responses to Psychotic Prompts (JAMA)

- "OpenAI's large language model (LLM)–based chatbot product ChatGPT has seen rapid adoption since its 2022 release. At least 28% of US adults have used it, most often for advice or tutoring.[1] The chatbot interface, which presents user prompts and LLM model outputs as messages and responses, can implicitly lead users to attribute comprehension and empathy to the product.[2] As responses are generated through pattern matching and alignment to user input,[3] they may accept inaccurate premises or reinforce the content of a user's message.[4] Recent media reports have described individuals in whom psychotic symptoms apparently developed or worsened in exchanges with ChatGPT, which appeared to echo or encourage unusual ideas.[5] In this cross-sectional study, we tested whether ChatGPT can reliably generate appropriate responses to psychotic content."
- TAKE-AWAY – the three different versions of ChatGPT showed high rates of inappropriate or partially appropriate responses to psychotic prompts, with the free version performing the worst.

# Recent Regulations, Opinions & Pending Cases

# Texas SB1188

- Texas Governor Abbott signed into law legislation (S.B. 1188) that regulates three main items:

(1) security of health record data;

(2) storage of health data overseas; and

(3) deployment of artificial intelligence (**AI**). The effective date is September 1, 2025 (or January 1, 2026 for the data localization requirement) and essentially, the law emphasizes electronic health record requirements and authorizes civil penalties.

# Texas SB1188 (AI Requirements)

**Regarding AI, the law requires the following:**

- Disclosure to patients by providers, their use of AI for diagnostic purposes;
- Utilization of AI is limited to the scope of a provider's license, certification or authorization;
- AI deployment is not otherwise restricted or prohibited by applicable state or federal law; and
- Review by the provider of all records created with AI in a manner consistent with medical records standards developed by the Texas Medical Board.

# Investing in the age of AI: What health care companies and investors need to consider.

**RVR: During our recent conversation, you mentioned a prudent example of LLM being utilized with a finite set of "good data," with a human verifier in relation to an epilepsy application. Can you expand on why this is an ideal application of AI and the positive benefits to patients?**

**BJL:** A good example is brain monitoring, in-hospital or at-home. There is a finite population of EEG monitoring techs. Typically a given tech is monitoring N numbers of EEG screens at a given time. The EEG data are clean, dense and continuous — all qualities that you want for a data source for use by AI/ML.

By using the target event (epileptic seizure) to train the data, you produce a clinical support system (Class II) that can be used by an EEG tech to significantly increase the number of patients monitored by a single tech. When the system is triggered by an EEG alert, the tech checks the data and confirms/rejects the imminent occurrence of a seizure. Thus you have a significant productivity tool that lets you (the tech) safely monitor a larger number of patients at any time. The tech (human) is calling the clinical shot here; the AI/ML is providing him with the alerts.

The prime benefit here is to the provider, allowing the provider to monitor a larger number of patients at a given time. This is important as there is a chronic shortage of EEG techs in the industry. It certainly reduces the monitoring cost. It is not at all clear that the provider passes that savings to the patient and/or payer.

# OpenAI hit with lawsuit claiming ChatGPT acted as an unlicensed lawyer.

- *Nippon Life Insurance Company of America v. OpenAI Foundation, et al.*, Case No. 1:26-cv-02448 (NDIL (Mar. 4, 2026)).
  - ChatGPT maker OpenAI has been accused in a new lawsuit of practicing law without a U.S. license and helping a former disability claimant breach a settlement and flood a federal court docket with meritless filings.
  - Nippon alleges that OpenAI wrongfully provided legal assistance to a woman who sought to reopen a lawsuit that was already settled and dismissed.
  - "ChatGPT is not a lawyer." the lawsuit said. Although OpenAI has shown ChatGPT can pass an attorney bar exam, Nippon said, "it has not been admitted to practice law in the State of Illinois or in any other jurisdiction within the United States."
  - The lawsuit appears to be one of the first cases to accuse a major AI developer of engaging in the unauthorized practice of law through a consumer-facing chatbot.
  - Nippon said the woman last year uploaded an email from her then-lawyer into ChatGPT, which allegedly validated her concerns about the advice she was being given. The woman fired her lawyer and moved to reopen her closed case using ChatGPT, the lawsuit said.

# *United States of America v. Heppner*, 25-cr-00503-JSR (SDNY (Feb. 2026)).

- Documents generated through a public AI platform were **not** protected by the attorney-client privilege or the work product doctrine.
- Specifically, the Court granted the Government's motion to access documents that defendant Bradley Heppner created using the AI tool Claude before his arrest on federal fraud charges.
- Government Arguments:
  - **The AI Documents were not communications between Heppner and his counsel**. Rather, they were made between Heppner and a public AI tool that is not an attorney. The Government analogized Heppner's use of Claude to him asking friends for input on legal matters, an act that does not create privileged communications.

# Terms & Conditions Highlights

# *Heppner* & The Government's Argument

- **The AI Documents were not created for the purpose of obtaining legal advice from counsel**. Specifically, Claude's "Constitution," terms of service, and other public materials expressly disclaim Claude's ability to give legal advice and instead suggest that the user consult with a qualified lawyer.
- **The AI Documents were not confidential**. Rather, Heppner voluntarily shared his prompts with a third-party commercial AI platform that is publicly accessible. Claude's Privacy Policy explicitly advises users that it collects data on prompts and outputs, uses this data to train its AI tool, and may disclose this data to governmental regulatory authorities and third parties.

# Strategies for Combatting Risk

# *Blueprint for an AI Bill of Rights*

- Five Principles

  (1)Safety and effectiveness

  ***(2)Algorithmic discrimination protections***

  ***(3)Data privacy***

  (4)Notice and explanation

  (5)Human alternatives, consideration and feedback

  https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/#:~:text=To%20advance%20President%20Biden's%20vision,or%20access%20to%20critical%20needs.

# NIST Frameworks

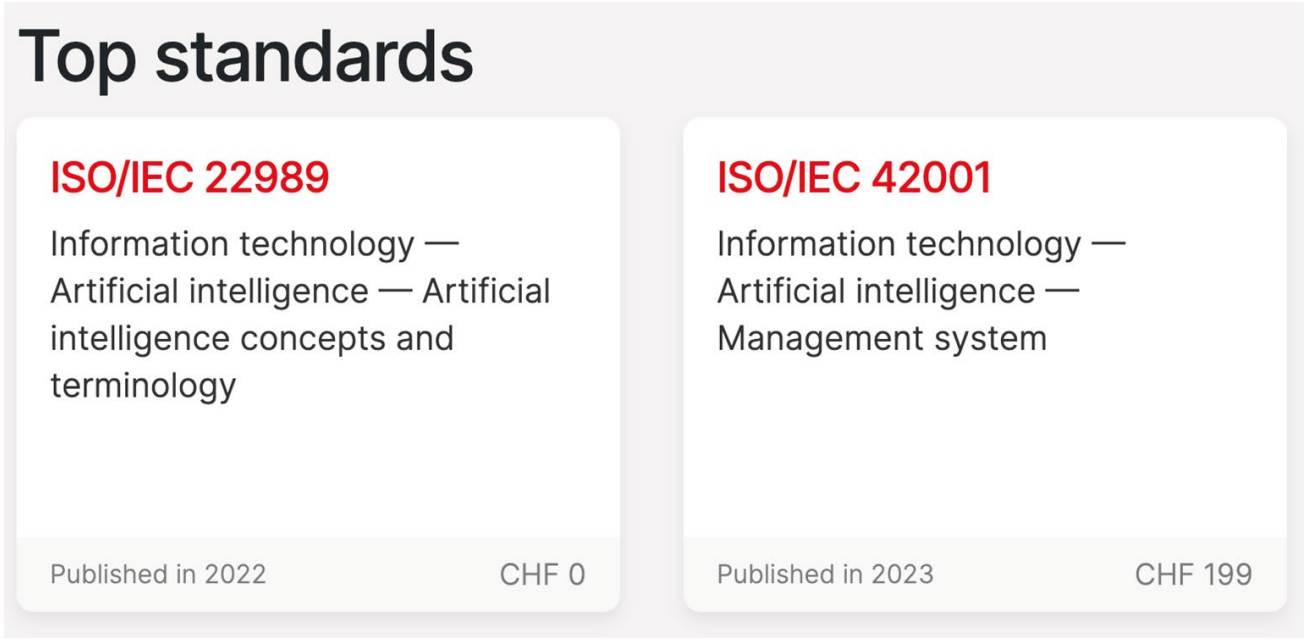
**Key Cybersecurity & Privacy Frameworks:**

- Cybersecurity Framework (CSF 2.0)
- Privacy Framework (PF 1.1)

**Key AI Standards:**

- AI Risk Management Framework (AI RMF 1.0) - NIST AI 100-1
- Secure Software Development Practices - NIST SP 800-218A
- Generative AI Profile - NIST AI 600-1
- Guidance on Synthetic Content

# ISO Standards & Certifications




**ISO/IEC 27001:2022 (amended)**
Information security, cybersecurity and privacy protection Privacy information management systems

**ISO/IEC 27701**
Information security, cybersecurity and privacy protection Privacy information management systems

# Learning from *Heppner*.

- **Communications with public AI tools may not be privileged**. Communications with public AI tools may not satisfy the requirements of the attorney-client privilege because AI tools are not attorneys, do not provide legal advice, and inputs to them are not confidential. Further, later sending the AI-generated results to a lawyer will not retroactively cloak them with privilege.
- **Public AI tool privacy policies are important**. Courts may examine whether AI tool privacy policies permit disclosure of user data to third parties and governmental authorities when evaluating confidentiality claims so such policies should be carefully reviewed prior to use of the AI tool.
- **Sharing privileged information with a public AI tool might waive privilege**. Taking the ruling a step further, it is reasonable to also conclude that sharing confidential attorney-client communications with a public AI tool might waive any privilege that could otherwise attach to those communications.

# Conclusion & Questions

# Conclusion

- Both ChatGPT and Claude claim to not engage in the practice of law or medicine. This is an area of case law to watch because only a human being can hold a law license or a medical license.
- To ensure that AI is safe, legal and ethical, use the *Blueprint*'s five factors.
- Include language in patient-provider agreements and attorney-client agreements related to AI.
- Know the type of software that is being evaluated.
- A human checker is critical.

# Thank You & Questions

Rachel V. Rose – Attorney at Law, PLLC

(713) 907-7442 * www.rvrose.com

**Blog** | **Articles** | April 2, 2026

# Investing in the age of AI: What health care companies and investors need to consider

*Author(s)* *Rachel V. Rose, JD, MBA*

*Fact checked by:* *Austin Littrell*

*Vanderbilt professor and health care entrepreneur Bruce J. Lynskey breaks down what companies and investors need to know before betting on AI in medicine.*



*Rachel V. Rose, J.D., MBA*

Artificial Intelligence (AI) is now common in everyday vernacular, including health care wellness apps and in providers' offices and facilities. Equally known is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the

requirements of confidentiality, integrity and availability — basically privacy and security of health data and individually identifiable health information (IIHI).

What should companies, providers, patients and investors be considering in relation to AI? First, what type of AI is being deployed — Generative AI (GenAI), ambient AI, agentic AI, and/or large language models (LLMs)?

Second, what safeguards are in place to ensure confidentiality, safety, non-discriminatory impact, appropriate notice to users or patients, and is there a human checking the information before the individual receives the answer or a claim is submitted for payment with codes that were AI-generated?

Third, is the application substantive or more like a dot.com era company that had a lot of promise but no substance behind it and led to the bursting of the dot.com bubble in the early 2000s?

In order to answer these types of questions, I reached out to a professor of mine, Bruce J. Lynskey, who has extensive health care and tech industry experience, as well as holding positions as a professor and adjunct professor at a variety of schools including

Vanderbilt University's Owen Graduate School of Management, where I was fortunate to take a number of classes from Prof. Lynskey.

**Rachel V. Rose, J.D., MBA: Throughout your career, in addition to teaching entrepreneurship classes at Vanderbilt's Owen Graduate School of Management, you have worked in both tech start-ups and co-founded a health care start-up with a successful exit. How does what's happening with the AI landscape compare to the Dot.com and telecom market bubbles?**

**Bruce J. Lynskey:** The dot.com and telecom market bubbles closely followed each other — a genuine two-fer. Very many of today's AI players and the investors were not yet born, just born, or children, so they have no experience going through one of these periods: significant rapid gains in the public and private markets followed by a bursting of the market. Companies large and small perished in these events. One graphic example is a fiber optics tech start-up did its IPO with $10M in revenue, all from one customer, and no profit.

The IPO stock was priced at $38/share. When the first shares traded on the public market at noon on a Friday, the opening

price was $250+ per share and rapidly increased, eventually reaching into the 400s. When the market correction occurred, with little warning, the stock plummeted to $3+ per share.

This telecom market collapse happened due to the over buildout of the fiber optic transmission infrastructure. There was a whole lot of idle 'dark fiber' in the ground with no data to transport. It took years for this to completely correct — the arrival of voice data, then music data, and finally video data. Is something analogous happening with the AI data center buildout?

In the current market we have severely inflated valuations of many AI related firms and scant evidence of proven business models. Some of the largest players are offering user prices that are substantially below their breakeven points to attract users. When they eventually are forced to raise their prices to something more sustainable, we will get to see the market (users') evaluation of the value of that service.

These characteristics of the AI market are identical to those of the dot.com market as

environmental impact, data centers' impact on inflating electricity prices, etc.), something that is certainly not going to help them when the going gets rough.

**RVR: What are the main differences that you're seeing with the application of AI in health care compared to the application of Dot.com in the health care sector nearly 25 years ago?**

**BJL:** With the dot.com on the consumer front, numerous health care focused sites emerged early including WebMD.com. These very useful sites (health care information for those seeking it) were dispensing health information to consumers. As they evolved, they became more sophisticated and ultimately served as inspiration for the numerous healthcare consumer apps that sprouted on the smartphones. Medical systems (Cleveland Clinic, Mayo Clinic, etc.) created patient facing sites that dispensed invaluable health care information.

On the business front, it took little time before health care (and other organizations) developed their own 'intranets' — internal internets restricted to employees. These intranets, coupled with a burgeoning software application industry, allowed


## Trending on Physicians Practice

1. How one health system turned data chaos into a 90% drop in report requests
2. What ChatGPT Health means for your patients and practice
3. Investing in the age of AI: What health care companies and investors need to consider
4. AI, layoffs and the law, with Christopher S. Mayer, J.D., of Frier Levitt
5. Introducing 'The Back Office'

organizations to automate their operations and achieve significant efficiencies. And yes, this automation resulted in reductions in staff and reassignments just as we are beginning to experience with the roll out of AI.

And yet, in spite of these technology-based transitions in the health care sector, the US health care sector still significantly lags its counterparts in other nations that have been working with 100% 'digital' health care environments for several years.

Current AI-driven applications are steadily making inroads in the clinical environment. Specialized chatbots are being used for intake, triage and initial patient assessment. In behavioral health, some AI is being used to provide behavioral therapy. There are virtual care assistants to assist patients after joint replacement procedures.

Many clinical care providers, with the patient's permission, are using AI tools that listen in on a patient's visit, record the conversation and translate the recording to physician notes, which the physician reviews and edits before entering them into the patient EHR.

All of these AI tools are productivity enhancing tools which free up care providers' time, allowing them to spend

providers' time, allowing them to spend more time with patients rather than with paperwork. There will be plenty more, and the market will determine which ones create value and are worth the expense.

It is inevitable, as is the case with any new technology, that some of these clinical deployments — and perhaps some 'front office' deployments — will hit some landmines that will result in litigation.

It is better to try it out, understanding that it is a new thing, and watch for and mitigate landmines, rather than believing it is possible to identify and erect all of the necessary fences in advance. We learn as we go.

**RVR: From your perspective and experience, how is AI being applied judiciously and how is it being applied recklessly in the health care sector?**

**BJL:** Many players are not aware that the U.S. health care industry was one of the early adopters of AI, and that occurred more than ten years ago. Some of the first deployments of AI occurred with imaging applications within health care. Diabetic retinopathy is a great example. Smart retinal scanners appeared that could scan the eyes and render a diagnosis, all in less than a few

minutes with a level of accuracy equal to or exceeding that of an ophthalmologist. These scanners are in wide usage today. Other imaging based applications followed.

At least ten years ago, the FDA started working with the EU to define and develop a new category of 'system' for the anticipated surge of AI-based clinical applications. They called the new category 'Software as a Medical Device' (SaaMD) and eventually created three classes (I, II, III) within the category.

In very general terms, Class I comprises consumer applications, Class II comprises clinical decision support systems, and Class

III comprises applications that take the place of humans making the decisions.

The highest risk area here is Class I, in that plenty of AI firms are deploying consumer health care apps without rigorous vetting or FDA approval. I call this the highest risk area because there are no guardrails. A company can build and release whatever it wants to the unsuspecting consumer and be liable for any adverse events.

One company is piloting its (Class I) consumer health care app (picture expert system) with a select group of users. It's good to see how users react and how and

why they use it.

A medical expert at a highly respected institution 'tested' the app with a series of serious medical symptoms and discovered that in 40% of the cases the test app failed to make the proper recommendation to the user. My purpose of citing this is to highlight the need to robustly test the application clinically.

In the cases of Class II and III systems, the health care providers serve as the primary guardrails. They are not going to deploy

anything without giving it careful vetting and ensuring that it is FDA certified or in the process of certification.

**RVR: During our recent conversation, you mentioned a prudent example of LLM being utilized with a finite set of "good data," with a human verifier in relation to an epilepsy application. Can you expand on why this is an ideal application of AI and the positive benefits to patients?**

**BJL:** A good example is brain monitoring, in-hospital or at-home. There is a finite population of EEG monitoring techs. Typically a given tech is monitoring N numbers of EEG screens at a given time. The

EEG data are clean, dense and continuous — all qualities that you want for a data source for use by AI/ML.

By using the target event (epileptic seizure) to train the data, you produce a clinical support system (Class II) that can be used by an EEG tech to significantly increase the number of patients monitored by a single tech. When the system is triggered by an EEG alert, the tech checks the data and confirms/rejects the imminent occurrence of

a seizure. Thus you have a significant productivity tool that lets you (the tech) safely monitor a larger number of patients at any time. The tech (human) is calling the clinical shot here; the AI/ML is providing him with the alerts.

The prime benefit here is to the provider, allowing the provider to monitor a larger number of patients at a given time. This is important as there is a chronic shortage of EEG techs in the industry. It certainly reduces the monitoring cost. It is not at all clear that the provider passes that savings to the patient and/or payer.

**RVR: In light of hallucinations, potential legal liability and, at times, the reckless application of AI, what should companies be doing to assuage investor**

**concerns and what should investors be doing in terms of due diligence before investing?**

**BJL:** First, understand if the 'product' directly interacts with the patient. If yes, then in what manner? Specifically, is it at all possible for the product to render a completely false response that may have negative consequences with the patient?

There already are countless LLM based products like this in the market. There is potential legal liability with these products.

Determine if your product needs to go through FDA certification. Most, if not all, clinical products do. If so, is it Class I, II or III? In all cases you should employ a quality management system (QMS) or equivalent right from the start, as you will need to submit significant information about the product along with the actual product (methodology, algorithms, etc.).

Investors should be literate with all of these issues prior to making an investment decision.

**RVR: Are there any macro-economic factors that both companies and investors should consider when setting their respective expectations and any historical events and/or types of**

**investors that are relevant?**

**BJL:** Three factors that are relevant here for companies and investors are:

**(1)** In the U.S. AI market, there is a significant amount of circular investing taking place in which A invests in B, with B committing to purchase services from A. This is setting up what will be a domino effect when the market starts deflating. Those firms who are involved with profitable, robust businesses will take a hit but will survive. Not the case with the other firms.

In these situations investors flee from the highly speculative firms to those with proven business models. You can think of it as the role in college that the Organic Chemistry course plays in quickly weeding out the viable pre-meds from the riff raff.

There was dramatic 'cleansing', small and large firms, in the dot.com and the telecom bubbles, followed by the investors heading for the hills, writing down investments and shedding staff.

**(2)** The U.S. market, the world's biggest, can tend to be provincial and not appreciate what's coming down the pike in other countries. Assume that all emerging and developed countries are immersed in AI development, and anything can emerge. The

development, and anything can emerge. The market is still very immature.

In the health care sector, prior to AI, there were market leading applications that were

developed in other countries (UK and India are great examples) a few years before any U.S. firm developed the same. Note that India has a significantly higher AI usage among its 1.4B population than does the U.S.

**(3)** Are we even using the optimal models and assumptions?

How do you know?

Are you sure?

## Conclusion

With the AI landscape continually involving, providers, patients, consumers, companies and investors have a lot to digest on a regular basis. Regardless of one's role, evaluating the safety, legality and ethics of a particular application is critical. Being realistic about the application, limitations and potential risks — whether legal, reputational or operational — are crucial to avoiding harm and a decreased valuation.

While large public companies have more of a buffer because of their product mix and market cap, smaller and private companies

could face a harder time weathering lawsuits, breaches and government enforcement actions. And, there are companies that are simply integrating ChatGPT or Claude to "create" a new technology without regard for intellectual property or laws such as HIPAA.

In sum, a reasonable investor should not be seduced by the allure of the shiny "AI" term, but instead understand the technology, relevant regulations and downstream risks.

***Rachel V. Rose, J.D., MBA**, advises clients on compliance, transactions, government administrative actions and litigation involving health care, cybersecurity, corporate and securities law, as well as False Claims Act and Dodd-Frank whistleblower cases. She also teaches bioethics at Baylor College of Medicine in Houston. Rose can be reached through her website, www.rvrose.com.*

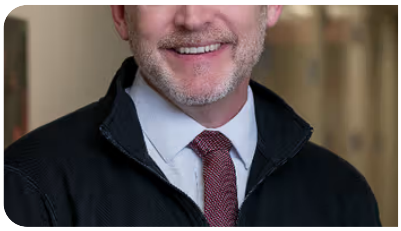
Physicians Practice Pearls® | Law & Malpractice | Technology & AI | HIPAA

## Related Content


### AI, layoffs and the law, with...

*By* Austin Littrell

April 2nd 2026



### How one health system...

*By* Keith A. Reynolds

April 1st


## What ChatGPT Health...

*By* Neil Baum, MD

April 1st 2026


## Introducing 'The Back Office'

*By* Keith A. Reynolds

March 31st 2026


## The war on health care fraud, wit...

*By* Austin Littrell

March 30th 2026

# Latest CME

In-Person + Virtual Event

**From Numbers to Navigation: Translating Data From Diabetes Technologies into Optimized Decision-Making**

April 16, 2026

View more



## Contact Info

259 Prospect Plains Rd, Bldg H
Cranbury, NJ 08512

609-716-7777