Significo

Ethics & Privacy in Personalized Healthcare:

Safeguarding Member & Employee Trust

Contents

In this digital age, emerging technologies offer a wealth of opportunities to improve and increase access to healthcare. However, they also pose potential risks to users' data privacy and raise a number of ethical questions about autonomy and consent that need to be addressed.

The use of personalization in health care solutions, for example, can be extremely effective for giving people greater understanding and control over their own health care — but only if users trust the solution and provider enough to input their health information.

When providing personalized healthcare solutions to members and employees, then, it's essential to be transparent about how their data will be used and to get their full, informed consent before they begin using the solution.

Keep reading to learn more about ethical and privacy concerns related to personalized healthcare solutions and how to safeguard member and employee trust while leveraging the benefits of personalization technologies.

Understanding Personalized Health Care & Privacy

Personalized health care solutions use the latest technologies to create a unique experience for each user. For example, solutions like Significo's SDK asks users to fill out questionnaires and then offers health improvement recommendations based on their answers.

These kinds of tools help users better understand their current health needs and plan their own health journeys. As a result, users gain:

Greater control over their health

Detailed insight into the current condition of their health

Information about available healthcare solutions

Easier access to health-related advice, data, and care

Deeper understanding of the uniqueness of their health journey

Additionally, by offering effective personalized health care solutions, organizations can demonstrate to their employees and members that each person's well-being matters and that their feedback is being heard and addressed.

However, personalized technology solutions come with a number of privacy concerns with regard to data collection, sharing, and security. Accurate personalization is possible only if the user provides detailed personal information, so it's imperative to protect that information and ensure users feel safe and comfortable providing it.

According to Benjy Silverman, Senior Scientific Consultant at Significo, helping users feel secure enough to provide their health information doesn't only mean preventing hacks or breaches. It also means reassuring them that the information they provide while using the solution won't be shared with their employer or other parties within the organization.

While at times it may be useful to share information with the individual's medical provider, it's important to consider how to enable that sharing without violating the person's ability to consent.

Addressing Ethical & Privacy Concerns

Health data is extremely sensitive, but personalized solutions rely on that data to perform effectively. So, it's imperative to collect, handle, and protect that data in an ethical, compliant, and consensual manner.

Ethical Considerations

Using technology to provide personalized health care can be a powerful way to ensure people from all walks of life have access to the care they need. However, certain ethical concerns must be taken into account to protect users from inaccurate information and inequitable practices.

"The biggest concern with anything that is based in machine learning or artificial intelligence, or is trying to provide recommendations that are not coming directly from a clinician, is that they could be wrong," Silverman says.

In this case, "wrong" can have one of two meanings:

- The recommendation, assessment, or diagnosis is incorrect
- The information is factually correct but delivered in the wrong way *(e.g., via a text alert instead of a face-to-face conversation)*

For this reason, Silverman advocates for using personalized health care tools as an extension of working with a clinician, rather than in place of one. Other ethical questions to consider when using technology for personalized health care include:

- Does the tool make health care more accessible and affordable?
- Has the tool been thoroughly tested for accuracy?
- What safeguards are in place to prevent the tool from potentially causing harm to users' health or privacy?
- Have users been clearly informed of how their data will be used?
- Are users fully aware of the potential risks of using the tool?

Instead of trying to tell people which decisions would be best for them, Silverman argues that it's important to give people all the information they need to make their own informed decisions — both in seeking or rejecting care and in using or abstaining from a certain piece of technology.

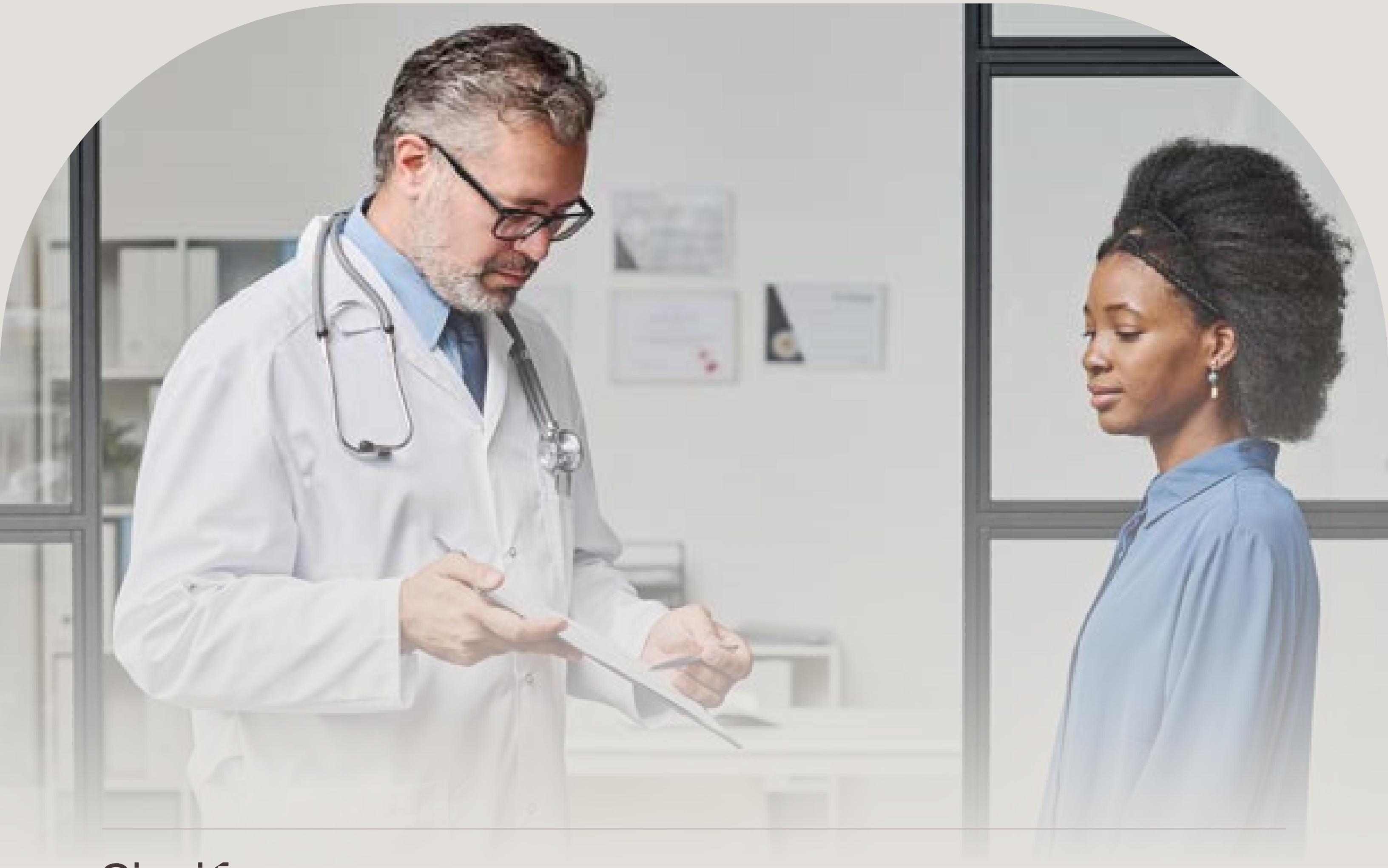
Privacy Safeguards

The Health Insurance Portability and Accountability Act (HIPAA) provides regulations for the protection of health data. However, unlike health companies, Silverman explains, “Most technology companies have not made that choice [to abide by HIPAA regulations] unless they’re going to work directly with health care companies.”

He notes that this isn’t because of the strictness of HIPAA standards. Rather, the barrier tends to be training and certification requirements. “It’s making a commitment to training the staff and to have 100% staff engagement on maintaining privacy and handling the data in an appropriate way,” he says.

In addition to HIPAA, other data compliance standards such as ISO 27001, Europe’s General Data Protection Regulation (GDPR), and SOC 2 by the American Institute of CPAs (AICPA) also demonstrate to consumers that the technology company can be trusted to safeguard their privacy.

“There are so many ways a person could misuse someone else’s medical data,” says Marc Herbertz, Significo’s Germany-based COO, naming blackmail and discrimination as two potential examples. “As a company, we are aware of this, and that’s why we’re adhering to all these established standards that people know they can trust.”



Implementing Ethical Solutions

When implementing personalized health care solutions, trust is key. And to establish trust, it's essential to address ethical and privacy concerns up front. "You have to take an ethics-first approach, because if people don't trust the tool or trust the people who make the tool, they're just not going to use it," Silverman explains.

However, defining and taking an ethical approach to privacy can be challenging, because not everyone is comfortable sharing the same amount of information online. While some people carefully guard as much of their personal information as possible, others don't even think twice about the amount of data they're sharing publicly.

Silverman recommends appealing to those who desire the greatest level of privacy. That way, those who don't care as much can simply agree to the terms and move on, while those who need more assurance have enough information to decide whether they feel comfortable using the tool.

Ultimately, taking an ethics-first approach to personalized health care means prioritizing transparency and informed consent. Silverman says, "With true informed consent, you are informing people of the risks and benefits. And the hope is actually that some people will say no." But, again, getting informed consent can be more complicated than it seems.

Requiring users to check a box acknowledging that they consent to the end-user license agreement may satisfy legal requirements, but it doesn't guarantee informed consent. Realistically, most people don't read a 50-page consent form. As a result, they have little to no understanding of what they're actually agreeing to.

To address this problem, Silverman suggests finding more digestible ways to communicate privacy policies and security measures. For example, instead of asking users to read a long block of text, consider presenting them with an interactive presentation with built-in knowledge checks to ensure they've absorbed the information.

The more transparent you are in communicating information about privacy and data use, the better-equipped people will be to either consent to or reject the terms of use — and the more confidently they will be able to trust that their data is safe in your hands.

Building Trust in Personalized Health Care

Herbertz points out that it's important to keep the end user in mind when providing personalized health care solutions. Not only do people need to feel safe and comfortable using the tool, but they also need to see how it positively impacts their well-being.

"We want to keep people safe and make their lives better," he says of Significo's SDK tool. "So the important part is not just the technical security but also the quality of the recommendations we offer." Of course, data security is also critical for keeping users safe and encouraging them to use the tool so they can achieve those positive outcomes.

That's why it's so important to build trust by complying with international privacy standards and communicating transparently about how you handle users' health data — because most people won't use the tool if they aren't confident that their information will be kept secure.

By clearly communicating how users' health data will be used, stored, and protected — and by following through on those promises — healthcare companies can build a reputation of transparency and reliability over time.

A 2020 survey by McKinsey found that while respondents were more likely to trust health care or financial services companies than businesses in other industries, less than 50% of respondents felt that healthcare companies could be trusted with their data privacy.

Additionally, roughly half of respondents were more inclined to trust companies that either didn't ask for more information than was necessary to use the service or product or were quick to respond to and publicly report data breaches.

By clearly communicating how users' health data will be used, stored, and protected — and by following through on those promises — healthcare companies can build a reputation of transparency and reliability over time.

Setting & Following Higher Standards

When it comes to setting and complying with ethical and security standards, Herbertz observes that technology often develops too quickly for legislation to catch up.

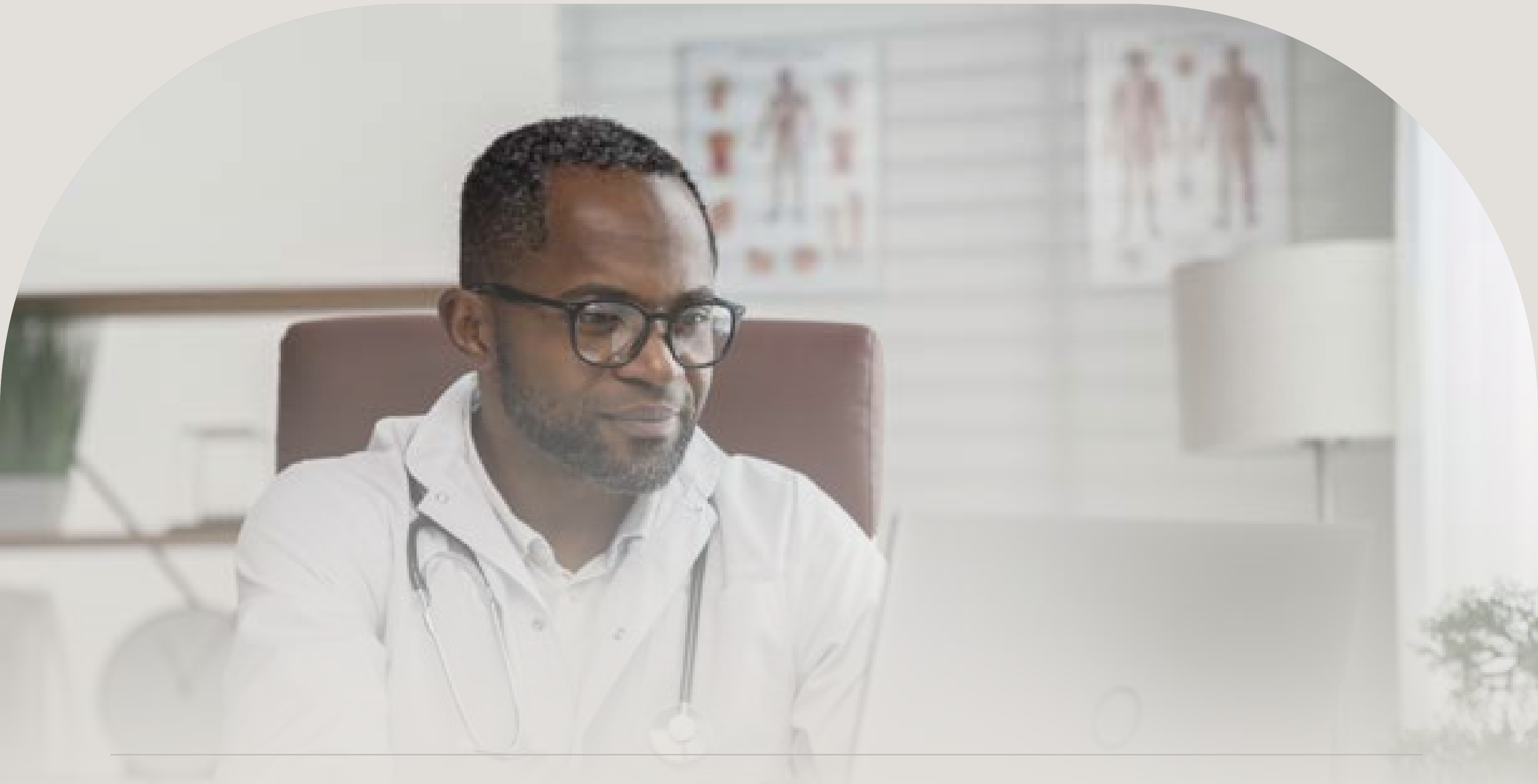
AI tools, for example, have been on the rise for the past few years. But much of the current legislation doesn't even address the use of AI, simply because at the time those standards were set, the only AI applications that existed were still too abstract for practical use.

This isn't an easy problem to solve because it's rooted in the established processes for writing and implementing legislation at national and international levels. Speeding them up incrementally would likely only serve to reduce the gap between the creation of new legislation and the development of new technology, not eliminate it altogether.

At a smaller, more localized level, technology development committees and organizations are engaging in dialogue with lawmakers to define and set regulations. Currently, however, individual companies don't have much, if any, influence on the creation of ethical and security standards for healthcare technology.

Instead, healthcare technology company leaders can help make following the established regulations as easy as possible for their employees and communicate why meeting those requirements is so important. After all, "You can say your product is secure, but the public won't trust you without proof that you actually have a secure product," says Herbertz.

In his experience, building a product that complies with international standards is more difficult and time-consuming than it would be otherwise and tends to be two or three times as expensive. The extra time, effort, and money, he concludes, is worth it to build a trustworthy product.



Protecting Privacy & Maintaining Confidence

Personalized healthcare solutions offer numerous benefits and opportunities for improved health outcomes, but they also come with certain ethical considerations and privacy concerns that must be addressed to build and maintain trust between organizations and end users.

By adhering to both national and international compliance standards and prioritizing transparency and informed consent, we can instill greater confidence in our personalized solutions to protect users' data and impact positive health outcomes.

At Significo, we're committed to empowering individuals to take control of their health — and their health data.

Schedule a demo to see what Significo can do for your organization.