CANNABIS NEWS YOU CAN USE
CANNABIS RISK MANAGER

Do Medical Cannabis Companies Need to Comply with HIPAA?

It's no secret that the federal government's original decision to classify marijuana as a Schedule 1 controlled substance was motivated more by politics than science. After over 50 years, the federal government is now on the cusp of rescheduling marijuana to Schedule 3, acknowledging the cannabis plant's numerous health benefits. This proposed shift represents progress in aligning federal marijuana policy with scientific understanding.

Intersection of Health Care and Data Privacy

While this potential rescheduling marks significant progress, it also raises new questions at the intersection of healthcare, data privacy, and cybersecurity.

HIPAA and Cannabis

The intersection between cannabis retailers and federal laws like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is complex. Whether a medical marijuana dispensary is a "covered entity" under HIPAA depends on if the dispensary is a "health care provider" and if it submits electronic claims to third-party payers.

Arguably, a medical marijuana (MMJ) dispensary qualifies as a health care provider under HIPAA, which defines healthcare as "care, services, or supplies related to the health of an individual." However, unless that dispensary also submits electronic claims for reimbursement, it is not a covered entity subject to HIPAA.

Medical Cannabis Claims

Typically, third-party payers, such as medical insurance companies, cover only "medically necessary" goods and services prescribed by a physician. While medical marijuana programs vary, most establish qualifying conditions that make patients eligible to use MMJ with a physician's recommendation. However, marijuana is not approved by the U.S. Food and Drug Administration (FDA) for medical use, meaning physicians cannot prescribe it for their patients.

Without FDA approval or changes in laws governing healthcare delivery and reimbursement, dispensaries will remain unable to submit electronic claims. This means dispensaries will continue to fall outside the definition of a covered entity, meaning they do not need to comply with HIPAA. Reclassification to Schedule 3 does not change this reality.

Protecting Privacy

While cannabis operators are likely not subject to HIPAA, that law is only part of the issue. Seventeen U.S. states now have privacy laws that apply to the collection, use, and disclosure of personal information. These

laws have strict requirements relating to privacy notices, data minimization, vendor management, and cybersecurity.

Cannabis companies collect a lot of data from their customers, including names, government IDs, payment-card information, photos, birthdates, addresses, phone numbers, and signatures. Reclassifying marijuana as Schedule 3 won't relieve state-mandated recordkeeping and reporting requirements, and increased research into the medical benefits of marijuana increases the risk that regulators will view the personal information collected by cannabis companies as health information.

Health Care Privacy

The Federal Trade Commission (FTC) and several states have identified a regulatory gap between HIPAA and non-HIPAA entities that process health-related information. Washington state's My Health My Data Act, for example, creates a private cause of action for noncompliance. Marijuana can be used recreationally or medicinally to treat health conditions, and a consumer's purchase of certain marijuana products might identify their health status, bringing dispensaries under the purview of such laws.

Cybersecurity Risks

Cannabis businesses are prime targets for hackers due to the sensitive data they collect. The risk is particularly acute for operators with mandatory seed-to-sale regulatory tracking requirements and retail point-of-sale software, both of which are often cloud-based. In 2023, 82% of data breaches involved data stored in the cloud. THSuites, a provider of dispensary software, experienced a vulnerability in 2020 that exposed 85,000 files containing customers' identifying information.

Rescheduling cannabis to Schedule 3 might not trigger HIPAA compliance, but data privacy regulation has already arrived for the cannabis industry. While the anticipated rescheduling likely will foster economic growth, it also brings increased data-privacy risks. Cannabis businesses would be well served to take their data privacy compliance seriously and conduct a review of their policies, vendors, and insurance coverage to prepare for the future.

Email: info@cannabisriskmanager.com | Phone: +415-226-4060