

## Data Privacy and Security in the Cannabis Industry

Article By:

Kathryn M. Rattigan

---

In November, cannabis won big in the midterm elections—in Michigan, the legalization of recreational cannabis passed, the legalization of medical cannabis passed in Utah and Missouri, and several states elected governors who back legislation for the legalization of cannabis. Now, there are 33 states that allow some form of medical marijuana and 10 states (plus D.C.) that have legalized recreational use. Additionally, the shift of the U.S. House of Representatives to Democratic control could also help the push for legalization at the federal level, as well as Attorney General Jeff Sessions' resignation.

So, while the industry is clearly on the rise as more and more states pass laws legalization the use of cannabis, the industry also needs to consider the privacy and security of its systems and networks from the ground up. Because this industry is so heavily regulated and tracked, there is also a heavy amount of data collection and storage of personally identifiable information and other sensitive data. Many businesses in this industry offer customers the ability to make purchases online or through a mobile app, use point-of-sale (POS) systems for their dispensaries and maintain their data on cloud-based software-as-a-service (SaaS) platforms. These POS systems automatically report to states' compliance tracking systems using application programming interfaces (APIs), and all of a business's daily sales can be uploaded automatically into the state's database in one simple step. In many instances, the dispensary scans their customers' ID for birth date and state of residency, and to check them into the system and confirm what (and how much) the customer can buy. When you think about it, marijuana dispensaries are hot spots for personally identifiable information –the goal is to track every plant, product, and person associated with the production and sale of marijuana.

Additionally, many of the same threats apply to the cannabis industry as those that affect all other businesses that are collecting data—use of public wi-fi by employees, loss of paper records, connected smart devices to your company's network, email and phishing scams. Cannabis businesses may want to consider implementing enterprise-wide data privacy and security compliance programs so that they have proper, up-to-date security measures in place, appropriate data breach response processes and adequate employee training. It is not only important for companies in the cannabis industry to keep up with the constantly-changing legislative landscape but also with the cyber threats that pose a substantial risk to their businesses and their customers, too.

Source URL: <https://natlawreview.com/article/data-privacy-and-security-cannabis-industry>