

## The Importance of Data Privacy in Cannabis Businesses By Cameron Wade

The pace of legal change in data privacy and cannabis has been well documented.<sup>1</sup> As these shifting regulatory schemes have each individually created headaches for businesses, it should come as little surprise that the intersection between them—ensuring adequate data privacy protection in state legal cannabis companies—poses particular compliance and logistical challenges. Cannabis and data privacy are each relatively new areas of law and are among the most active areas of legislation at the state level.<sup>2</sup> The difficulty of maintaining compliance in this dynamic regulatory environment is enhanced by the variance of regulations between states. Three states have comprehensive data privacy laws, however even these laws offer varying levels of data protection.<sup>3</sup> There are significant differences in compliance requirements between states without comprehensive data privacy laws, such as Ohio, and California, where privacy law is the most stringent in the United States.<sup>4</sup> State cannabis laws are similarly varied and range from fully legal adult use (18 states) to total illegality (4 states) with multiple degrees of partial legality in between.<sup>5</sup>

Cannabis businesses sit at an intersection between these two changing and varied areas of law because of the quantity of sensitive consumer information these companies are responsible for protecting. Cannabis dispensaries acquire vast troves of information, including payment card information, driver's license card numbers, dates of birth, addresses, phone numbers, medical ID card numbers, email address, and signatures.<sup>6</sup> An additional layer of precaution must be reserved for medical cannabis programs, which fall under the heightened scrutiny of the federal Health Insurance Portability and Accountability Act (HIPAA) and state equivalents.<sup>7</sup> Under medical cannabis programs, states generate a list of medical conditions which qualify a patient for cannabis treatment.<sup>8</sup> These conditions are typically quite serious and include terminal illnesses and illnesses which impose severe chronic pain.<sup>9</sup> This information is protected by HIPAA, and because medical cannabis dispensaries must store this sensitive health information in order to

---

<sup>1</sup> See Joyce E. Cutler, *Cannabis Practices Sprout as Big Law Firms Follow the Money*, BLOOMBERG (Sept. 21, 2021, 6:01 AM), <https://news.bloomberglaw.com/business-and-practice/cannabis-practices-sprout-as-big-law-firms-follow-the-money>. See also Detlev Gabel & Tim Hickman, *The Rapid Evolution of Data Protection Laws*, ICLG, <https://iclg.com/practice-areas/data-protection-laws-and-regulations/1-the-rapid-evolution-of-data-protection-laws> (last accessed Jan. 16 2022).

<sup>2</sup> Chris Hart & Jeremy Meisinger, *Cannabis Data Privacy Issues to Watch in 2021*, BLOOMBERG (Feb. 9, 2021, 4:00 AM), <https://news.bloomberglaw.com/privacy-and-data-security/cannabis-data-privacy-issues-to-watch-in-2021>.

<sup>3</sup> Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>.

<sup>4</sup> HART & MEISINGER, *supra* note 2.

<sup>5</sup> DISA, *Map of Marijuana Legality by State*, (Jan. 2022), <https://disa.com/map-of-marijuana-legality-by-state>.

<sup>6</sup> Daniel R. Stoller, *Law Firms Growing Cannabis Practices With Privacy Cases in Mind*, BLOOMBERG (Dec. 27, 2018, 6:31 AM), <https://news.bloomberglaw.com/privacy-and-data-security/law-firms-growing-cannabis-practices-with-privacy-cases-in-mind>. See also Bethany Moore, *Member Blog: As Cannabis Sales Rise, So Do Questions About Privacy and Security*, NATIONAL CANNABIS INDUSTRY ASSOCIATION (Feb. 4, 2021), <https://thecannabisindustry.org/member-blog-as-cannabis-sales-rise-so-do-questions-about-privacy-and-security/>.

<sup>7</sup> STOLLER, *supra* note 6.

<sup>8</sup> HART & MEISINGER, *supra* note 2.

<sup>9</sup> *Id.*

provide cannabis to patients, these companies are responsible for protecting the data as specified by federal rules.<sup>10</sup> Many states clarify that consumer and medical information must be stored for multiple years, which creates immediate and enormous data protection responsibilities for cannabis companies.<sup>11</sup> In 13 states and Washington D.C., these companies are also required to report large amounts of data to METRC (Marijuana Enforcement Tracking Reporting Compliance).<sup>12</sup> Many of these states require companies to carefully track cannabis products through the entire supply chain.<sup>13</sup>

Even without these difficult data privacy regulatory burdens, the regulation of cannabis companies presents them with perplexing and expensive challenges, and even companies with the best intentions have been known to struggle with compliance because of unclear and rapidly changing regulations.<sup>14</sup> The broadly dispersed compliance challenges in the cannabis industry can have the effect of distracting companies from properly implementing data privacy protection measures. Over the past five years, cannabis companies have suffered breaches which have exposed sensitive medical and financial information of thousands of customers and patients.<sup>15</sup> Although data privacy compliance can be expensive, the costs of these breaches are steeper to patients and dispensaries alike. Data privacy breaches are a problem for any business, but they expose cannabis companies to the additional risk that government officials in states which are opposed to cannabis legalization may use breaches as an excuse to target out-of-state cannabis companies.<sup>16</sup> Cannabis breaches can also present heightened problems to consumers. In addition to violations of privacy and financial risks associated with breaches in other industries, cannabis breaches can expose consumers to the reputational risks associated with lingering stigmas surrounding cannabis transactions.<sup>17</sup> Although the regulatory climate is murky, varied, and constantly changing, it is imperative that sensitive information is adequately protected in the cannabis industry.

---

<sup>10</sup> STOLLER, *supra* note 6.

<sup>11</sup> MOORE, *supra* note 6.

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> HART & MEISINGER, *supra* note 2.

<sup>15</sup> Matthew R. Kittay, *Data Breach Exposes Cannabis Industry Security Vulnerabilities*, FOX ROTHSCHILD LLP (Feb. 25, 2020), <https://www.foxrothschild.com/publications/data-breach-exposes-cannabis-industry-security-vulnerabilities>.

<sup>16</sup> STOLLER, *supra* note 6.

<sup>17</sup> KITTAY, *supra* note 15.