Health Information Portability and Accountability Act (HIPAA) - Privacy

For Medical and Same Site Cannabis (dispensaries with both Medical and Adult Use licenses at the same location licensed and regulated by the IDFPR) (Updated June 2021)

Under the Compassionate Use of Medical Cannabis Program Act – A 280. dispensing organization shall ensure that any identifying information about a qualifying patient, provisional patient, OAPP participant or caregiver is kept in compliance with the federal privacy and security rules of HIPAA (45 CFR 164).

1. **What is HIPAA compliance?**
   Health Information Portability and Accountability Act (HIPAA) is a federal and state mandate requiring healthcare entities to keep patient's data protected. Compliance requires numerous of privacy and security action such as: password policy creation, patient data protection, and agent training.

2. **What is a Covered Entity (CE)?**
   Any business entity that must by law comply with HIPAA regulations, which include healthcare providers, insurance companies, and clearinghouses. In this context, health care providers include doctors, medical, dental, vision clinics, hospitals, medical cannabis dispensaries and related health caregivers including agents who work within medical cannabis dispensaries.

3. **What is a Business Associate (BA)?**
   An entity that receives patient data from either a covered entity, or from another business associate. An example is a call center that handles patient calls for a medical licensed cannabis dispensary organization. The call center practices must be HIPAA compliant, if not, the medical licensed cannabis dispensary organization will be fully liable for the actions of the call center.

4. **What is Personally Identifiable Information (PII)?**
   Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.[i] PII includes common identifiers such as: name, address, social security number, date of birth, or any other information that can be used to identify the individual.

5. **What is Protected Health Information (PHI)?**
   Privacy Rule protects all "individually identifiable health information" held or transmitted or maintained by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Information collected by a covered entity relating to the past, present or future health or condition of an individual and must be protected.[ii] PHI is a subset of PII. Some PHI examples include: medical records, facial photo, and cannabis allotment limits.

6. **Types of PHI include?**
   Protected health information is information, including demographic information, which relates to:[iii] the individual's past, present, or future physical or mental health or condition, the provision of health

care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

7. **Who is responsible for HIPAA?**
   Healthcare entities including medical cannabis dispensaries and its individual staff members who accesses PHI are responsible for HIPAA privacy and security. Entities are responsible to implement necessary safeguards to ensure HIPAA compliance for medical cannabis patients. Individuals and entities can face civil and/or criminal charges for mishandling PHI.

8. **Who is required to become HIPAA compliant?**
   Any covered or business associate including medical cannabis dispensaries that stores, processes, transmits, maintains, or handles protected health information in any way must be compliant.

9. **Does HIPAA extend to medical-use cannabis?**
   Yes. Any 280.dispensary organization, or organization that works with a 280.dispensary organization that collects, processes, stores, or transmits PHI about a customer is bound by HIPAA. Examples include: a medical cannabis dispensary who uses a website to process online orders (include 3rd party websites) or processes payments electronically through their point-of-sale system.

   Delivery organization are seen as a BA who delivers directly to medical patients are held to HIPAA regulations. In the delivery of products to medical cannabis patients, the equipment must be encrypted, documents and forms must be destroyed/shredded appropriately and photos must be stored securely.

10. **What's the difference between the HIPAA Security and Privacy rules?**
    Privacy Rule addresses appropriate PHI use and disclosure practices by healthcare entities. Security Rule addresses safeguarding the systems that store and/or transmit PHI utilized by healthcare entities including medical cannabis dispensaries.

11. **When is PHI required to be disclosed by a medical cannabis dispensary:**
    A medical cannabis dispensary must disclose protected health information in only two situations:
    to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and
    to IDFPR when it is undertaking a compliance investigation or review or enforcement action.

12. **Can I disclose a medical cannabis patient PHI over the phone or email?**
    Yes. If the medical cannabis patient or their designated caregiver(s) contact their medical dispensary and request information including their allotment or product information, the medical dispensary must disclose requested information directly pertaining to the patient. Communicating to medical cannabis patients via email must be encrypted.

13. **When is PHI permitted to be used and/or disclosed by a medical cannabis dispensary:**
    A covered entity may use and/or disclose protected health information, without an individual's authorization, for the following purposes or situations:
    - Treatment, Payment, and Health Care Operations;

- Opportunity to Agree or Object;
- Incident to an otherwise permitted use and disclosure;
- Public Interest and Benefit Activities; and
- Limited Data Set for the purposes of research, public health or health care operations
- Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make**.**

14. As a medical cannabis dispensary agent, can I discuss PHI to others including coworkers, other dispensaries or healthcare providers including designated caregivers?

Yes. You are covered in sharing that information during the course of a patient's treatment, payment or operations exemption seen in the federal statute. If the sharing of PHI is not in the assistance for a patient's care or not covered under a federal exemption, then it is a HIPAA violation.

15. As a medical cannabis dispensary agent, can I discuss PHI to the patient's family members?

Yes. The patient does have the right to object with the information being shared, however, the medical cannabis dispensary may rely on their best judgement when sharing that information to family members or caregivers in the care of the medical cannabis patient.

16. Is a medical cannabis dispensary required to distribute a "Notice of Privacy Practices for Protected Health Information"?

Yes. The Privacy Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information about the individual, as well as his or her rights and the covered entity's obligations with respect to that information. Most covered entities must develop and provide individuals with this notice of their privacy practices.[iv]

17. What information is required for the "Notice of Privacy Practices for Protected Health Information"?

Covered entities are required to provide a notice in plain language that describes:

- How the covered entity may use and disclose protected health information about an individual.
- The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity.
- The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information.
- Whom individuals can contact for further information about the covered entity's privacy policies.
- The notice must include an effective date. See 45 CFR 164.520(b) for the specific requirements for developing the content of the notice. A covered entity is required to promptly revise and distribute its notice whenever it makes material changes to any of its privacy practices. See 164.520(c)(2)(iv) for covered health care providers with direct treatment relationships with individuals.[v]

18. When is the medical cannabis dispensary required to provide the "Notice of Privacy Practices for Protected Health Information" [vi] **?**

- A covered entity must make its notice available to any person who asks for it.
- A covered entity must prominently post and make available its notice on any website it maintains that provides information about its customer services or benefits.

- Provide the notice to the individual no later than the date of first service delivery (after the April 14, 2003 compliance date of the Privacy Rule) and, except in an emergency treatment situation, make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If an acknowledgment cannot be obtained, the provider must document his or her efforts to obtain the acknowledgment and the reason why it was not obtained.
- When first service delivery to an individual is provided over the Internet, through e-mail, or otherwise electronically, the provider must send an electronic notice automatically and contemporaneously in response to the individual's first request for service. The provider must make a good faith effort to obtain a return receipt or other transmission from the individual in response to receiving the notice.
- In an emergency treatment situation, provide the notice as soon as it is reasonably practicable to do so after the emergency situation has ended. In these situations, providers are not required to make a good faith effort to obtain a written acknowledgment from individuals.
- Make the latest notice (i.e., the one that reflects any changes in privacy policies) available at the provider's office or facility for individuals to request to take with them, and post it in a clear and prominent location at the facility.
- A covered entity may e-mail the notice to an individual if the individual agrees to receive an electronic notice. See 45 CFR 164.520(c) for the specific requirements for providing the notice.

19. How do I become HIPAA compliant?

Administer a comprehensive risk analysis (at least annually), conduct a risk management, conduct employee training (at least annually), and implement updated policies and procedures.

20. When do 280. licensed dispensaries need to be compliant with HIPAA regulations?

For notice of Privacy Practices for Protected Health Information be available for patients no later than August 1st, 2021. Complete security risk assessment and compliance with encryption of electronic devices and networks (computers, tablets, websites, etc.) should be no later than December 1st, 2021.

21. Does 280. licensed dispensaries have to hold evidence of delivery of Notice of Privacy Practices for Protected Health Information to medical cannabis patients?

Yes, 280. dispensaries are responsible for retaining proof of delivery to medical cannabis patients for a minimum of 5 years. Notice of Privacy Practices for Protected Health Information can be delivered in written or electronic form.

22. Who enforces HIPAA compliance?

The Illinois Department of Financial and Professional Regulation is the State agency responsible for enforcing HIPAA compliance for dispensaries who hold a medical cannabis dispensary license.

23. What are the penalties for HIPAA non-compliance?

Fines can be issued through citation (maximum $10,000 per violation) or sent to prosecutions. Fees and penalties can be assessed on either the agent, dispensary or both.

24. What is a HIPAA violation?

Each failure to follow one or more of the HIPAA standards, requirements, or implementation specifications is considered a violation. HIPAA violation examples seen in medical cannabis dispensaries include: sharing computer passwords, discussing PHI to outside 3rd parties, not using an industry-standard firewall, not encrypting computers or networks where data is transmitted and/or

stored, not encrypting emailed patient data, not disclosing PHI from requested patient. These are all separate violations and can lead to enforcement actions from the IDFPR.

25. Am I expected to conduct a HIPAA audit?

Yes. IDFPR expects dispensaries who hold a medical cannabis dispensary license to actively work on their HIPAA compliance and tests them through audits (at least annually). An entity could be chosen for a HIPAA compliance audit at random, or because of a reported breach by an agent or patient. Noncompliance can lead to enforcement from the IDFPR.

26. How is a HIPAA Breach defined?

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.[vii]

27. Are there any exceptions to a HIPAA breach?

Yes. There are three exceptions to the definition of "breach."[viii]

- The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
- The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
- The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

28. If a HIPAA breach occurs at my medical cannabis dispensary or with any of my business associates, an I required to notify my medical cannabis patients?

Yes. Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information:[ix]

<u>Individual Notification 1-500 impacted patients:</u>

- Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by encrypted, secured e-mail if the affected individual has agreed to receive such notices electronically.
- If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.
- The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
- If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

Individual Notification over 500 impacted patients (include Media):
Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction within 60 calendar days following the discovery of a breach and must include the same information required for an individual notice.

29. **If a HIPAA breach occurs at a medical cannabis dispensary or with any business associates, must IDFPR be notified?**
Yes. Medical cannabis dispensaries must notify IDFPR of breaches of protected health information. Medical cannabis dispensaries will notify IDFPR by emailing FPR.MedicalCannabis@Illinois.gov and DPH.MedicalCannabis@Illinois.gov. In the subject area of the email indicate HIPAA Breach and include medical dispensary name and license number. Notification must occur no later than 60 calendar days following the discovery of the breach.

30. **If my BA actions causes a breach of my medical cannabis patient information, which party is responsible for notifying both IDFPR and my affected patients?**
With respect to a breach at or by a business associate, the covered entity is ultimately responsible for ensuring individuals and IDFPR are notified. The covered entity may delegate the responsibility of providing individual notices to the business associate.[x]

31. **When must a medical cannabis dispensary notify its medical cannabis patients of a HIPAA breach?**
Notifications must be provided without unreasonable delay and in no case later than 60 calendar days following the discovery of a breach.[xi]

32. **What information is required in HIPAA breach notifications to medical cannabis patients?**
Notifications, in plain language, must include, to the extent possible:[xii]
    - a brief description of the breach,
    - a description of the types of information that were involved in the breach,
    - the steps affected individuals should take to protect themselves from potential harm,
    - a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, and
    - contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

33. **Should IDFPR be notified when computers are stolen from a medical cannabis dispensary?**
Yes. Contact the IDFPR immediately, within 24 hours, following discovery of the theft. Email FPR.MedicalCannabis@Illinois.gov and DPH.MedicalCannabis@Illinois.gov. In the subject area of the email indicate HIPAA Breach and include medical dispensary name and license number.

DISCLAIMER: The above questions and answers are provided for general information only and may not be completely accurate in every circumstance, do not purport to be legal advice, and are not intended to be legally binding on the Department in a particular case. Questions involving interpretation of the law and your legal rights and obligations should be addressed to your lawyer.

---

[i] OMB Memorandum M-07-16
[ii] 45 CFR § 160.103
[iii] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#_edn2
[iv] 45 CFR § 164.520
[v] 45 CFR § 164.520
[vi] 45 CFR § 164.520

[vii] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[viii] 45 CFR § 164.402
[ix] 45 CFR § 164.404
[x] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[xi] 45 CFR § 164.404(b)
[xii] 45 CFR § 164.402(c)