FAQs

Health Information Portability and Accountability Act (HIPAA) - Security

For Medical (280) and Same Site Cannabis Dispensaries (dispensaries with both Medical and Adult Use licenses at the same location)

Under the Compassionate Use of Medical Cannabis Program Act - A 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 privacy and security actions such as: password policy creation, patient data protection, and agent training.

2. **What HIPAA Security standard "safeguards" comprised of?**

   HIPAA security is comprised of 3 areas for compliance: Administrative, Physical and Technical standards. Those can include: setting up separate networks for systems carrying confidential data, forcing log outs and other standard security practices.

3. **What are Administrative safeguards?**

   Safeguards examples include: security management process, assigned security responsibility, workforce security, information access management, security awareness training, security incident procedures, contingency plan and evacuation.

4. **What are Physical safeguards?**

   Safeguards examples include: facility access control, workstation use, workstation security and device and media controls.

5. **What are Technical safeguards?**

   Safeguards examples include: access control, audit controls, integrity controls, person or entity authentication and transmission security.

6. **What is Security Risk Analysis?**

   Medical cannabis dispensing organizations should conduct a risk analysis to determine the appropriate security measures. That assessment should include:

   - Identify areas of high security risk for E-PHI
   - Evaluate likelihood and impact of the risks
   - Implement security measures to address the risks
   - Document the measures and their rationale

7. **Where can I locate someone to conduct a Security Risk Analysis?**

   The Department does not recommend any vendors; however, it is strongly recommended that a qualified HIPAA Security consulting firm conducts the analysis initially and then annually. IDFPR will be using Security Risk Analysis reports to confirm encryption of electronic devices holding e-PHI.

8. **Does HIPAA require encryption of patient information (e-PHI)?**

   Yes, HIPAA requires the encryption of patient information when stored on a disk, hard drive, tape, USB drives, and any non-volatile storage. This is called encryption of data at rest.[i] HIPAA also requires the encryption of data as it moves across a network via a web browser session, FTP or any other method used to transfer data. This is called encryption of data in motion.[ii] This would include all websites used to for medical cannabis patient online orders.

   The encryption of patient data provides acceptable protection to both medical cannabis patients and the medical cannabis dispensary organization. It's the only defensible strategy in light of how the Department will evaluate a data breach that may occur.

9. **Should IDFPR be notified when non-encrypted computers are stolen from a medical cannabis dispensary?**

   Yes. Contact the IDFPR immediately, within 24 hours, following discovery of the theft. Email DPH.MedicalCannabis@Illinois.gov and FPR.MedicalCannabis@Illinois.gov In the subject area of the email indicate HIPAA Breach and include medical dispensary name and license number.

10. **If medical cannabis dispensary computers are encrypted, rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals, do I have to report to IDFPR the stolen computers?**

    No, it is not required for you to report the theft of the encrypted computers to the IDFPR, however, it is strongly encouraged.

11. If medical cannabis dispensary experiences a breach with their network (encrypted or unsecured) should IDFPR be notified?

Yes. Email DPH.MedicalCannabis@Illinois.gov and FPR.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.

12. 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 annually.

13. **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**.

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] 45 CFR 164.312(a)(2)(iv)
[ii] 45 CFR 164.312(e)(2)(ii)