64ER22-7 MMTC Websites and Website Purchasing.

(1) For the purposes of this rule, the terms below shall have the following meanings:

(a) "Personal identifying information" means data which includes, but is not limited to, the patient's or caregiver's name, social security number, email address, address, date of birth, photograph, and telephone number.

(b) "Website" means a group of webpages made available online through the internet.

(c) "Website purchasing" means the purchasing of or making reservations or pre-reservations for the purchasing of usable product or marijuana delivery devices by a qualified patient or caregiver through an MMTC's department-approved website.

(2) An MMTC shall have only one website, which must be approved by the department. The department-approved website must contain the information enumerated in s. 381.986(8)(i), F.S.

(3) An MMTC must obtain department approval for its website, and any changes or additions (i.e., redirects) to the website URL, by submitting a completed form DH8037-OMMU-08/2022, "Request for Website or Website Purchasing," incorporated by reference herein and available at https://knowthefactsmmj.com/rules-and-regulations/.

(4) An MMTC's department-approved website must have a mechanism to verify that each visitor is either 18 years of age or older or a qualified patient before allowing the visitor to access the MMTC's website.

(5) An MMTC may only offer website purchasing on the MMTC's department-approved website.

(a) An MMTC must obtain approval from the department prior to offering website purchasing by submitting a completed "Request for Website or Website Purchasing" form. With its request for approval, the MMTC must also submit documentation evidencing the MMTC's compliance with the standards enumerated under paragraph (5)(b) below.

(b) An MMTC must ensure that personal identifying information obtained in the website purchasing process remains confidential. To ensure all personal identifying information remains confidential, an MMTC must comply with the following security standards:

1. The MMTC must secure the user interface of the website using Hypertext Transfer Protocol Security (HTTPS) to ensure that the data transfer between the user and server is secured with Transport Level Security Protocol (TLS) and Secure Socket Layer Cryptographic Protocol (SSL).

2. The MMTC must use an anti-virus system to prevent software intrusions on the servers and MMTC computers that access the MMTC's servers. The anti-virus system must be updated regularly and must utilize the most current version.

3. The MMTC must utilize a firewall that employs network monitoring and intrusion detection systems at the server level and that deploys intrusion prevention systems at the server level.

4. The MMTC must employ a system that will authenticate all website users who access website purchasing information and that will assign access privileges based on each user's specific permissions. The ability to access information on the MMTC's website must be limited to the scope of the user's specific permission level.

a. For MMTC employees, the ability to access information on the MMTC's servers must be limited to the scope of the individual's specific permission level, which must be based on the employee's duties. Privilege levels for employees must be reevaluated by the MMTC every three months to ensure appropriate access.

b. The MMTC must maintain records of all system access. These records must be made available to the department within 48 hours of the Department's request.

5. The MMTC's servers must be housed in a secure location, which may include a data center. Such secured location must be Standards for Attestation Engagements (SSAE) System and Organization Controls (SOC) Type III certified.

(c) Prior to collecting personal identifying information for purposes of website purchasing, the MMTC must obtain express consent from the patient or caregiver permitting the MMTC to use their information for that purpose. Once the consent has been received, the MMTC must ensure that personal identifying information is not used for any other purpose.

(d) Upon becoming aware of any data breach that includes personal identifying information obtained in the website purchasing process, an MMTC shall:

1. Immediately notify patients and caregivers affected, or potentially affected, by the breach; and

2. Submit a written corrective action plan to the department within seven days of the incident. The corrective action plan must include, at a minimum, the action steps the MMTC intends to take to correct the data breach, the specific deadlines for each action step, and the additional steps the MMTC intends to take to prevent a data breach in the future.

(e) Nothing in this rule is intended to relieve an MMTC of its obligations to comply with federal and state laws and regulations for data security and breach notification.

(f) An MMTC must comply with s. 381.986(8)(e)16., F.S., when dispensing usable product or marijuana delivery devices through website purchasing.

(6) An MMTC may only dispense usable product and marijuana delivery devices sold through in-person purchases at the MMTC's dispensing locations; telephone purchases directly between the MMTC's employees and the patient or a caregiver; or website purchasing under this rule.

(7) An MMTC that currently offers website purchasing must comply with the provisions of this rule and submit a completed "Request for Website or Website Purchasing" form within 60 days of the effective date of this rule.

(8) An MMTC with an existing department-approved website must submit a "Request for Website or Website Purchasing" form with the website's current URL within 60 days of the effective date of this rule.

Rulemaking Authority Art. X, § 29, Fla. Const., 381.986(8)(k), F.S. Law Implemented Art. X, § 29, Fla. Const., 381.986(8)(h), 381.986(8)(i), F.S. History – New.