Utah Department of Health & Human Services

# Electronic verification system (EVS) health information privacy training

## Introduction

This training is for medical provider proxies (also referred to as proxies). Proxies are employees of a medical provider or medical clinic who can review, edit (also called amend), and submit patient information in the electronic verification system (EVS) on the medical provider's behalf.

Utah law requires that all proxies complete training about health information privacy laws before you access the EVS and when you renew your proxy registration with the Utah Department of Health and Human Services (DHHS).

## What you'll learn

We will cover the following topics in this training:

- What the electronic verification system (EVS) is.
- What information you'll access in the EVS.
- When you can access information in the EVS.
- How to protect patient information in the EVS.
- The consequences of not handling patient information correctly.

Read this training and appropriate laws carefully! You and the medical provider you work for will be responsible for any violations of federal and state patient privacy laws.

## The electronic verification system (EVS)

### What is the EVS?

The EVS is an electronic system that manages medical cannabis patient cards and purchases. It includes personal information in each patient's account, including PII (personally identifiable information) and PHI (protected health information).

Patients must meet with their medical provider before they get a medical cannabis card. Their provider will review their health concerns and health history to figure out if medical

cannabis is a good fit for the patient. If the provider decides that the patient can use medical cannabis, they will enter a certification into the patient's EVS account.

This certification verifies that the medical provider met with the patient and determined that medical cannabis would be a good treatment option for them. Patients need a certification entered in their EVS account before they can get a medical cannabis card and start buying medical cannabis.

Medical providers can also submit dosing guidelines, called recommendations, that state the amount and types of medical cannabis the patient can buy.

A medical provider can update the patient's certification or recommendation with new information, or remove the certification if the patient doesn't need medical cannabis anymore.

The EVS will keep track of the patient's certifications, recommendations and notes from medical providers, purchases, and when their card expires.

**How will I use the EVS?**

There are 2 ways that you'll use the EVS as a proxy:

1. To review, edit, and enter information from the medical provider into patient EVS accounts. This information includes certifications, recommendations, and other notes. You can only make these changes when instructed to by the medical provider who certified the patient.
2. To help patients apply and renew for medical cannabis cards. With patient permission, you'll have access to create or update an EVS account and fill out a medical cannabis card application directly for them.

## Protecting patient information

**What laws do I need to follow about patient information?**

You must follow state and federal laws about protecting patient information. Take a minute to review each of these laws. We will summarize some of them through the rest of this training.

- Utah Administrative Rule R383-2-3
- Utah Code 26B-4-2-202(7-9)
- HIPAA laws

You and the medical provider will be responsible for any consequences of not following these laws. Consequences may include the following:

- Losing your proxy registration.
- Losing access to the EVS.
- Civil or criminal penalties, such as misdemeanor or felony charges.
- Fines up to $5,000.

You must also follow other policies and procedures that your medical provider or clinic uses to protect patient information.

**When can I access patient information in the EVS?**

Privacy laws state you can only access patient information if you have a legitimate business need for it.

Legitimate business needs can include the following situations:

- When you work with a patient directly to create an EVS account, submit a medical cannabis card application, or edit information in their account.
- When the medical provider tells you to enter or edit information in a patient's EVS account.
- When you're providing customer service directly to a patient about their EVS account or medical cannabis card.

**PII** is any data that can be used to identify, contact, or locate a person. It includes things like name, address, email address, birthdate, and social security number.

**PHI** is a type of PII that is specific to a person's health history, diagnoses, and treatments. It includes things like medical records, insurance claims, and lab results.

If your job duties change and you no longer need to access patient records, you will no longer have a legitimate business need to see patient information. You or your medical provider must remove your EVS access.

Privacy laws also state you should only access the minimum amount of information needed to complete the task. For example, if you don't need to see a patient's purchase history to enter a new certification in a patient's account, do not look at that information.

Utah Department of Health & Human Services

**How can I protect patient information in the EVS?**

Utah law states you must safeguard all patient information in the EVS by using these guidelines:

- Do not share patient information with anyone who doesn't have access to the information (such as family, friends, or even other coworkers).
- Do not share patient information with anyone—including coworkers—who don't need to know the information.
- Do not share your login information for the EVS with anyone.

**What are the privacy and security concerns?**

A privacy and security incident is an event that actually or potentially violates privacy and security policies and procedures or compromises information or an information system's confidentiality, integrity, or availability. This can include such things as accidentally losing or releasing information, or misusing information.

Follow these steps if there is a privacy incident or breach, even if it is just for 1 patient.

1. Tell the medical provider.
2. Email the DHHS Center for Medical Cannabis at qmpcmc@utah.gov.
3. Contact the patients whose information was released in the breach.

**Privacy incidents and breaches** can include situations such as:

- Sending an email with PII or PHI to the wrong patient on accident.
- Sharing information about a patient without the patient's lawful consent to a person who is not authorized to receive the information.
- Exceeding your authorized access by using information from a patient's account for something not related to their medical cannabis card.
- Hacking a software system, such as through phishing, malware, or ransomware attacks.

DHHS will tell you and the medical provider if there's anything else you need to do.

## Conclusion

Thank you for taking the time to read this document! Email qmpcmc@utah.gov if you have questions.