Best Practices in Managing User Accounts

HIPAA guidelines direct all covered entities and business associates to limit user access to protected health information (PHI) to the minimum necessary in order to accomplish their intended purpose, use, disclosure or request.

Kareo PM provides you several options to manage how users access and utilize the system. Understanding the level of access of each user to your system is the responsibility of the practice and it is a good idea to regularly monitor your user roles and permissions within Kareo PM to ensure HIPAA compliance. Below are FAQs regarding Kareo PM and Kareo EHR security.

**What is an ideal user setup for a typical Kareo PM practice?**

For most practices, it is sufficient to create a few user roles to meet the majority of needs, as well as create one primary user with the Account Administrator permission and one back-up.

Note that the Account Administrator will have access to all areas of the system and will also have the ability to create users and change permission levels. Setting up users with this level of access should be minimal for most practices.

Note that if you are using Kareo EHR, any user in Kareo PM with Account Administrator permission will also be an administrator in Kareo EHR. This was designed to simplify setup and access of administrators between the two systems. In most practices, this is the ideal configuration.

**How can I define the security access controls for my practice?**

The practice should define the access controls for the system to ensure that they meet all the requirements of their compliance plan.

To define your Security Policy Options, click Settings in the top menu, then Options and Security Policy Options.
If we use Kareo EHR, are all my Kareo PM users automatically created in my Kareo EHR?

To simplify creation of users in Kareo EHR, we automatically create and add the same users from Kareo PM to the Kareo EHR. Users can then use the same login credentials. However, only users that are assigned Account Administrator permission will initially be able to access your Kareo EHR. All other users will have to first be assigned an appropriate role in the Kareo EHR by the Kareo EHR Account Administrator before they can access any areas in Kareo EHR.

We currently have a billing service and we see all their users in our Kareo EHR – are they able to access our Kareo EHR?

Your billing service should have created a specific role for their billers with a custom permission to allow them to access the minimum necessary to perform their tasks. As long as none of the users have been granted Account Administrator permission, they will not be able to access your Kareo EHR until they are assigned a user role within Kareo EHR.

What else should I do to ensure that users in my system are only accessing areas appropriate to their job function?

At Kareo, we find that many practices are very “liberal” in granting access to their users. This is especially true with the Account Administrator permission. Limiting user access to the minimum to allow them to perform their job will go a long way to limiting inappropriate access. Also, if you took the time to create roles when setting up your system, it is a good idea once you learn more about the different features of Kareo to revisit and fine-tune the roles.