Mass General Brigham

PAS & KEYGIVING: KEYGIVER RESPONSIBILITES TIP SHEET

This guide provides an overview of Keygiver responsibilities related to viewing and managing access to network resources using the Personnel Authorization System (PAS).

Managing Access

Keep in mind that some of the systems or SFAs managed in PAS contain patient information, financial, or other protected data. Users should only be given the *minimum level of access* required to perform their job. All access given to or removed from a user is tracked in their **Audit Log**.

Granting Access

- You should only grant access to users in your department/project team.
- If needed, find other Keygivers who may be more appropriate to assign access using the:
  - Keygiver Search report in PAS
  - Department Keygiver Directory

Removing Access

- Remove access when no longer needed, such as when an employee transfers to a new department.
- In most cases, system and SFA access is removed when someone leaves the Mass General Brigham network entirely.

Confidentiality

Some confidential user information can be found in PAS.

As a Keygiver you should:

- Only view and search for users on a need-to-know basis
- Always search for users by user name
- Shred any screenshots or printed reports

Helpful Security Reminders

- Never share your passwords
- Always lock your device when stepping away:

Quarterly Audit

Keygivers are required by HIPAA, along with Mass General Brigham privacy and security policies, to perform a regular review of the system and SFA access they manage. This audit should be completed quarterly. An email reminder is sent to Keygivers every 90 days.

Audit Instructions

1. Generate an **Account List** report for each system and SFA you manage.
2. Remove users who no longer need access.
3. Confirm the rights for each user are still appropriate and adjust them if necessary.

If applicable, you should also:

- Ensure the content stored in your SFAs is appropriate for users who have access.
- Review access to systems *not* managed in PAS, e.g. SharePoint or other department-specific programs.

Note: You do not need to include systems that are part of the Clinical Systems Audit.

ⓘ Additional Support & Training Information

View the full Keygiver Reference Guide in article KB0036812 or contact the Digital Service Desk.