

# Fade to Lock for effective walk-away security

Solving the unattended workstation problem

## Improve walk-away security without impacting caregiver productivity

As regulatory requirements continue to grow, hospital IT teams must find ways to help care providers meet their compliance responsibilities without impacting their productivity.

Imprivata Fade to Lock technology does exactly that. It gives care providers a smarter and more efficient way to handle security and privacy for a common and particularly challenging reality in their workflows – the unattended workstation.

## The growing need

Interruptions are part of the job for most healthcare providers. But when clinicians need to step away, they might not log off properly from their EHR applications or their desktops. These situations result in unattended workstations, which present a range of privacy and security risks. Among them:

- Care providers inadvertently charting under the wrong ID
- Patients' safety and privacy put in jeopardy
- Hospitals exposed to risk of HIPAA violations and other regulatory infractions

The traditional approach for securing unattended workstations is a time-out and automatic screen lock. But time-outs are inflexible. Settings that are too short disrupt clinical workflows. Too long, and they fail to provide the needed security and privacy. Given the seriousness of the risks and the productivity problems caused by time-outs, it's time for a new approach to walk-away security. Fade to Lock provides a new and innovative way for hospital IT teams to meet their walk-away security challenges.

## Benefits

- Avoids costly and damaging charting errors
- Improves workstation security
- Protects patients' privacy
- Improves care providers' productivity

## The optimal balance of access and security

Fade to Lock is a feature of Imprivata Enterprise Access Management with single sign-on (formerly Imprivata OneSign®). It utilizes intelligent time-out settings that can vary based on whether the care provider is using, or has logged out of the EHR. By gradually fading the screen after a period of inactivity, Fade to Lock provides a warning to care providers that their workstation will be locking shortly. A keyboard click or nudge of the mouse reopens the screen to full view, enabling care providers to avoid repetitive and time-consuming logins while remaining in their patient workflows. Prominent display of the logged in user's name on the Fade to Lock privacy screen helps care providers avoid charting under the wrong ID.

**By gradually fading the screen after a period of inactivity, Fade to Lock provides a warning to care providers that their workstation will be locking shortly.**

## Fade to Lock benefits

**Avoids costly and damaging charting errors:** In addition to obscuring the open session behind it, the Fade to Lock privacy screen prominently displays the name of the currently logged in user. When another provider arrives at that shared workstation, he or she sees only the other user's name and knows immediately that they need to log in properly.

**Improves workstation security:** The Fade to Lock privacy screen obscures a workstation's display to prevent inappropriate exposure of protected health information (PHI). This is an especially valuable feature for shared workstations located in publicly accessible areas.

**Protects patients' privacy:** With steep financial penalties and reputational damage resulting from HIPAA violations and data breaches, hospitals are challenged to secure PHI while enabling fast access for those who need it. Fade to Lock is designed specifically to protect PHI without impacting clinical workflows.

**Improves care givers' productivity:** By gradually obscuring screens rather than abruptly locking them down, Fade to Lock passively warns the clinician that their session will soon time-out. With a nudge of the mouse, the clinician can reopen the view of their session. The fading screen helps care providers avoid wasting time and getting frustrated with excessive log ins.

## Fade to Lock technology – a closer look

By utilizing technology enabled by Imprivata Enterprise Management (EAM), Fade to Lock recognizes when a provider is using the EHR or other clinical applications. As patient interactions will create periods of inactivity with the EHR even though the provider is still present, a longer time-out can be set. The gradual fade to the privacy screen gives the provider plenty of warning without obstructing access to information and can be easily cleared with a key press or nudge of the mouse. If the fade goes uninterrupted, the screen will become completely obscured by the Fade to Lock privacy screen. This protects PHI on the workstation from accidental viewing, displays the name of the user who is logged in to prevent accidental access, and can still be cleared by the mouse or keyboard. After a period of time, the workstation will lock, requiring re-authentication. When the provider

logs out of the EHR, a much shorter time-out can be set for both the privacy screen and the final locking of the workstation should the provider have forgotten to log out of the workstation. All time-out settings are policy controlled through the EAM Administration console and set by workstation or group. Fade to Lock requires no extra hardware and fully supports both physical and virtual environments.

## Conclusion

For care providers to stay productive while meeting increasing compliance requirements, they need fast and easy access to information. But patients' PHI needs to be safeguarded effectively. For hospital IT teams, balancing the opposing needs for information access and security is an ongoing challenge, especially with walk-away situations.

The Fade to Lock functionality, and the broader technology of EAM, protect hospitals, providers, and patients' privacy by providing the optimal balance of information access and security.

The Fade to Lock functionality, and the broader technology of EAM, protect hospitals, providers, and patients' privacy by providing the optimal balance of information access and security.



Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at:

**Global headquarters USA**

Waltham, MA

**Phone:** +1 877 663 7446

[www.imprivata.com](http://www.imprivata.com)

**European headquarters**

Uxbridge, England

**Phone:** +44 (0) 208 744 6500

[www.imprivata.com/uk](http://www.imprivata.com/uk)

**Germany**

Langenfeld

**Phone:** +49 (0) 2173 99 385 0

[www.imprivata.com/de](http://www.imprivata.com/de)

**Australia**

Melbourne

**Phone:** +61 3 8844 5533