

Can you prove who is looking at your sensitive healthcare data?

Ensure the verified and authorized user accessing your sensitive or regulated data is the same person being authenticated throughout an active session, **and no one else**, while also protecting the user's privacy.



Cybersecurity Risk Mitigation

People and data are an organization's primary assets. The need to protect both the individual and data, especially in a hybrid working environment, has never been more critical. Healthcare data has an extremely high value, making healthcare organizations targets for cyberattacks. Reduce the risk of unauthorized access to the data by limiting access to only known personnel on approved devices and approved locations, throughout an active session, thus extending physical security controls to the hybrid working environment.

Why SessionGuardian for Healthcare Organizations

SessionGuardian ensures that only authorized users on an authorized device from an authorized location can access a VDI or web asset via SessionGuardian VDI and SessionGuardian Web. Our use cases include protection against stolen/lost laptops, stolen credentials, improper security safeguards and secure third-party service provider access.

SessionGuardian for Healthcare Organizations Benefits

HIPAA Compliance

Protected Health Information (PHI) contains highly sensitive demographic information, medical histories, social security numbers, insurance information, and financial information. Knowing that the person who is authorized to view the data is actually accessing that data at all times is key to remaining HIPAA compliant. This is especially true in the work-from-anywhere paradigm. Our continuous facial authentication confirms that an authorized user is "who they say they are", and applies additional security restrictions throughout the entire session of access, not just at login.

Insider Threat Avoidance

Insider threats are a significant issue for any organization. This is especially true where sensitive HIPAA-related data is at risk. By applying configurable security controls, such as user identity, device, and location as factors of authentication, the probability of malicious (credential sharing, shoulder surfing, mobile phone photos) or accidental (transfer of private PHI) insider threats is vastly reduced.



IDENTITY ASSURANCE

- Facial Authentication - Continuous or One-Time
- User Present/Liveness Detection
- Shoulder Surfing Prevention
- 3rd Party ID Verification
- SSO Integration

DEVICE ASSURANCE



- Verify Device Integrity
- Known Networks (IP/VPN Restrictions)
- Geolocation Approve/Deny
- Allowed/Unauthorized Applications
- Time of Day

DATA PROTECTION



- Prevent Screenshare, Screen Capture, Screen Print, File Download
- Detect Mobile Phone to Prevent Screen Photo
- Watermarks

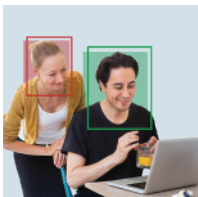
PRIVACY COMPLIANCE



- No Biometric Data Stored or Transmitted
- Compliant with All Major Privacy Regulations Including GDPR and HIPAA
- Granular Audit Trails
- Alerts
- SIEM Integration

Enhance Security Protocols for Your Sensitive Healthcare Data

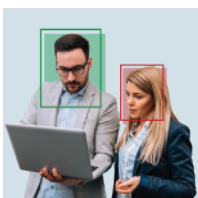
Extend physical security controls to your third-party and remote/hybrid healthcare organization with SessionGuardian's continuous identity verification solution to protect Virtual Desktop Infrastructure (VDI) and web-based applications.



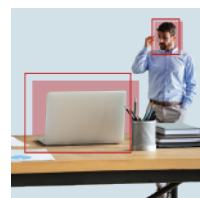
SHOULDER SURFING
How do you prevent an unauthorized person from shoulder-surfing?



PHOTO OF SCREEN
How do you prevent a screen shot of sensitive data?



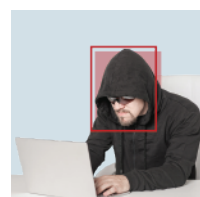
CREDENTIAL SHARING
How do you know that the person is using their own credentials to log in and not someone else's?



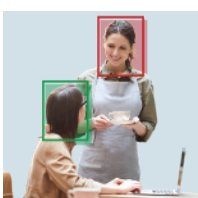
USER NOT PRESENT
How do you know that the person is truly present during the session?



eMEETING SHARING
How do you know your meeting attendees are authorized to see the screenshare?



CREDENTIAL HACKING
How do you know that the person (employee, contractor, partner or customer) logging in with legitimate credentials really is that person?



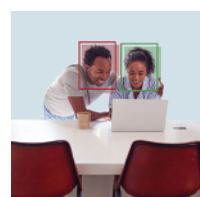
INCORRECT GEOLOCATION
How do you know the user is logging into your system from an authorized location?



COMPROMISED DEVICE
How do you know the user is on a healthy device that passed security requirements?



THIRD-PARTY ACCESS CALL CENTERS
How do you know that third parties with access to your data are in a physically secure environment?



REMOTE/HYBRID EMPLOYEES OVEREMPLOYMENT
How do you know that your remote employees are in a physically secure environment?

Protect Your Hybrid Environment

Our configurable security controls can be applied to your VDI or sensitive web applications, putting security at your fingertips. These controls are defined in a common control plane, managed by your organization, that facilitates the creation and assignment of the desired security posture to protect your VDI and web assets.

Global Privacy Compliance

Paramount to the design of SessionGuardian is the privacy of the end-user above all else. SessionGuardian complies with all major global privacy regulations, including HIPAA and GDPR. In addition to protecting your data, SessionGuardian also protects the privacy of your end-user.

Key Use Cases

Preventing unauthorized access to healthcare data is essential, and SessionGuardian can help. We enable you to limit access to your data by extending physical security controls to the hybrid working environment and allowing only authorized personnel from authorized devices in authorized locations. With SessionGuardian's solutions, you can secure:

- Remote BPOs accessing ePHI
- Remote BPOs sending PHI to patients/contacts
- Remote/hybrid staff accessing sensitive ePHI
- Protect patient data in a clinical environment

About SessionGuardian

SessionGuardian is the leader in continuous identity verification for third-party and remote/hybrid teams. Our cybersecurity solutions protect highly sensitive assets from data theft. We ensure that the verified and credentialed user, who is accessing your sensitive data, is the same person throughout the active session, while also safeguarding their privacy.

For more information about SessionGuardian and to schedule a demo, contact info@SessionGuardian.com.

