



## Keep Unwanted Eyes Off Your Sensitive Healthcare Data

Thank you for downloading this SessionGuardian brochure. Carahsoft is the distributor for SessionGuardian cybersecurity solutions available via ITES-SW2, NASPO ValuePoint, Educational Software Solutions and Services - OMNIA Partners, Public Sector, and other contract vehicles.

To learn how to take the next step toward acquiring SessionGuardian's solutions, please check out the following resources and information:



For additional resources:  
[carah.io/sessionguardianresources](https://carah.io/sessionguardianresources)



For upcoming events:  
[carah.io/sessionguardianevents](https://carah.io/sessionguardianevents)



For additional SessionGuardian solutions:  
[carah.io/sessionguardiansolutions](https://carah.io/sessionguardiansolutions)



For additional cybersecurity solutions:  
[carah.io/sessionguardiansolutions](https://carah.io/sessionguardiansolutions)



To set up a meeting:  
[sessionguardian@carahsoft.com](mailto:sessionguardian@carahsoft.com)  
571-662-3817



To purchase, check out the contract vehicles available for procurement:  
[carah.io/sessionguardiancontracts](https://carah.io/sessionguardiancontracts)

# Keep Unwanted Eyes Off Your Sensitive Healthcare Data

Defend your sensitive healthcare data with SessionGuardian's robust prevention of **unauthorized shoulder-surfing** and protection against **photographs being taken of screens**



VERIFIED  
COMPLIANT



## 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, web, mobile, or desktop asset via SessionGuardian. Our use cases include third-party and remote/hybrid employee access, contact centers, and legal document review.

## Benefits for Healthcare Organizations

### 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
- 3<sup>rd</sup> Party ID Verification

### 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



## 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 GDPR and HIPAA. In addition to protecting your data, SessionGuardian also protects the privacy of your end-user. Furthermore, SessionGuardian is SOC 2 and ISO 27001 certified.

## Key Use Cases

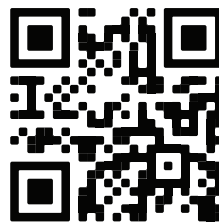
Preventing unauthorized access to healthcare data is essential, and SessionGuardian can help. We enable you to limit access to your data by extending physical security controls to the hybrid working environment and allowing only authorized personnel using approved and healthy devices from vetted locations. 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

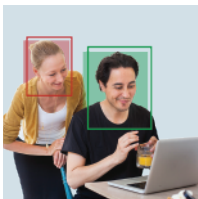
SessionGuardian is the leader in continuous identity assurance and data protection for third-party and remote/hybrid teams. Our cybersecurity solutions protect highly sensitive assets from data theft. We ensure that the verified and credentialed user, who is accessing your sensitive data, is the same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

For more information about SessionGuardian and to schedule a demo, contact [info@SessionGuardian.com](mailto:info@SessionGuardian.com).



# Enhance Security Protocols for Your Sensitive Healthcare Data

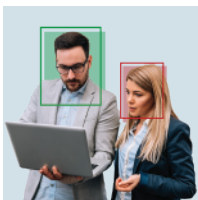
Extend physical security controls to your third-party and remote/hybrid teams with SessionGuardian's continuous identity assurance solution to protect VDI, web, mobile and desktop environments.

A woman in a yellow jacket is looking over the shoulder of a man in a black shirt who is using a laptop. Red and green bounding boxes highlight their faces.

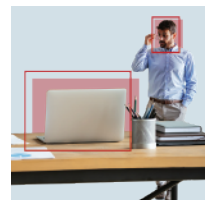
**SHOULDER-SURFING**  
How do you prevent an unauthorized person from shoulder-surfing?

A man in a blue shirt is sitting at a desk with a laptop. A red bounding box highlights his face, and another red bounding box highlights the laptop screen.

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

A man in a grey suit is showing a laptop screen to a woman in a blue jacket. Red and green bounding boxes highlight their faces.

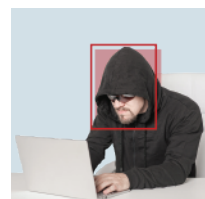
**CREDENTIAL SHARING**  
How do you know that the person is using their own credentials to log in and not someone else's?

A man in a blue shirt is standing behind a desk with a laptop. A red bounding box highlights his face, and another red bounding box highlights the laptop screen.

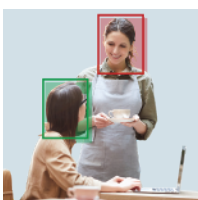
**USER NOT PRESENT**  
How do you know that the person is truly present during the session?

A person is pointing at a laptop screen displaying a meeting interface. A red bounding box highlights the person's face.

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

A person in a black hoodie is sitting at a desk with a laptop. A red bounding box highlights their face.

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

A woman in a grey dress is standing and talking to a man in a brown shirt who is sitting at a desk with a laptop. Red and green bounding boxes highlight their faces.

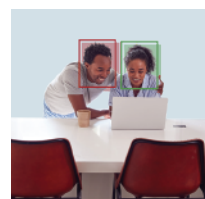
**INCORRECT GEOLOCATION**  
How do you know the user is logging into your system from an authorized location?

A woman in a yellow top is sitting at a desk with a laptop. A red bounding box highlights her face, and another red bounding box highlights the laptop screen.

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

A man in a grey suit is sitting at a desk with a laptop. A red bounding box highlights his face, and another red bounding box highlights a woman in a white shirt who is also at a desk with a laptop.

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

Two women are sitting at a table with a laptop. Red and green bounding boxes highlight their faces.

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