	Policy: Screen Lock Out	
	Department Responsible: PepperPointe IT	Date Approved:
	Effective Date: January 1, 2024	Next Review Date: January 1, 2025

Intended Audience:

Entire workforce

Scope and Goals:

This policy outlines the requirements and procedures for screen lock out settings across our organization. The primary objective is to safeguard sensitive information by ensuring that unattended computers, tablets and other screen connected devices automatically lock after a specified period of inactivity.

Responsibilities:

Workforce

- Adherence to Policy: Comply with the default 15-minute screen lock out policy.
- Locking Workstations: Manually lock computers when leaving the workstation unattended.
- Reporting Issues: Report any issues or difficulties with the screen lock out settings to the IT department promptly.
- Policy Acknowledgment: Read, understand, and sign the "Screen Lock Out Policy Acknowledgment Form."

Workforce Supervisor

- Enforcing Compliance: Ensure all team members adhere to the screen lock out policy.
- Approval of Requests: Review and approve any initial requests for an extended screen lock out period up to 30 minutes for clinical use.
- Monitoring Compliance: Regularly monitor and ensure compliance with the policy within their department.
- Policy Communication: Communicate the importance and requirements of the policy to all team members.

Information Technology Team (IT Team)

- Policy Implementation: Configure and enforce the default 15-minute screen lock out setting on all computers.
- Support and Troubleshooting: Provide support and troubleshoot any issues related to screen lock out settings.
- Review of Override Requests: Review and process requests for screen lock out period extensions beyond 30 minutes.
- Security Monitoring: Monitor systems for compliance with the screen lock out policy and report any violations.

COO/IT Leadership

- Policy Development: Assist in developing and updating the screen lock out policy as needed.

- Risk Assessment: Assess the risks associated with any requests for extended screen lock out periods.
- Review and Approval: Thoroughly review and approve/disapprove override requests for lock out periods beyond 30 minutes.
- Incident Response: Respond to any security incidents related to non-compliance with the screen lock out policy.

Human Resources (HR)

- Policy Documentation: Maintain records of signed "Screen Lock Out Policy Acknowledgment Forms."
- Disciplinary Action: Coordinate and implement disciplinary actions for staff members who violate the policy.
- Training and Awareness: Provide training and resources to staff members to ensure understanding and compliance with the policy.

Clinical Staff (Where Applicable)

- Extended Use Compliance: Adhere to the approved extended lock out period up to 30 minutes for clinical use cases.
- Special Requests: Submit formal requests for any required screen lock out period extensions beyond 30 minutes.
- Operational Security: Implement additional security measures to protect sensitive information during the extended lock out period.

Default Screen Lock Out Settings

- Default Inactivity Period:
  - All computers must automatically lock after 15 minutes of inactivity. This is the best practice to ensure security and protect sensitive data.

Clinical Use Case Extension

- Extended Inactivity Period for Clinical Use:
  - For specific clinical use cases where a 15-minute inactivity period is impractical, an extended lock out period of up to 30 minutes may be applied. This extension is granted to support clinical workflows that require longer active sessions without compromising patient care or operational efficiency.

Requesting a Special Override

- Override Request Procedure:
  - In exceptional cases where a lock out period beyond 30 minutes is required, staff must submit a formal request using the "Screen Lock Out Override Request Form."
  - The request form should include:
    - Justification for the extended inactivity period
    - Duration of the requested extension
    - Impact on workflows and patient care
    - Mitigating controls to ensure security during the extended period
- Review and Approval Process:

    - All override requests will undergo a thorough review by the COO and IT Leadership.
    - The review process will evaluate the necessity, potential risks, and mitigating controls outlined in the request form.
    - Approved requests will be documented, and the requesting department will be notified of the decision.

<u>Compliance and Disciplinary Actions</u>

- Policy Acknowledgment
    - All staff members are required to read, understand, and sign the "Screen Lock Out Policy Acknowledgment Form."
    - By signing, staff members agree to adhere to the policy and understand the importance of locking computers when not in use.
- Enforcement and Disciplinary Actions:
    - Failure to comply with this policy, including not locking computers when stepping away, may result in disciplinary action.
    - Disciplinary actions may range from warnings to termination of employment, depending on the severity and frequency of the violations.

<u>Conclusion</u>

The implementation of this Screen Lock Out Policy is crucial in maintaining the security and confidentiality of our organization's data. Adherence to this policy by all staff members will help ensure that sensitive information always remains protected.