forcura

# Health Information Security

## Recommended Best Practices

Whether a small agency without a dedicated information security position or a large organization with a team of experts, healthcare companies must not only fortify their digital systems against cyber attacks, but remain ever-vigilant of new threats and take proactive measures when needed. The following guidelines can assist you in your efforts; please note that this is not a definitive list, and you will want to comply with any obligations established by your security team or vendor.

- Notify leadership immediately regarding any unauthorized access to your company's systems or data.
- Notify leadership immediately of any employee termination that would require removal of authorized access to your company's systems or data.
- Periodically review user access lists to ensure appropriate role-based access to your company's systems is in place.
- Ensure that appropriate removal of authorized access to your company's systems or data is timely.
- Implement processes and controls to protect against security and availability threats from sources outside the boundaries of the system.
- Apply logical access to security controls, data encryption controls and related procedures for network-connected equipment.
- Protect equipment against malicious and unauthorized software/code.
- Comply with contractual obligations.
- Ensure that your company's end users have appropriate oversight, management, and control of systems or data.
- Ensure that procedures are in place for developing, maintaining, and testing business continuity and disaster recovery plans.
- Utilize only approved, encrypted communication (encrypted e-mail, SFTP, etc.) to convey sensitive data such as PHI to third parties.
- Notify leadership immediately if you discover compromised credentials for any accounts with access to your vendor's systems or data.
- Enforce appropriate password configurations relating to complexity, expiration, re-use/history, and lockout.
- Enforce inactivity timeouts on all workstations accessing your company's systems or data.

**To keep pace with the latest information regarding cyber security and best practices, also be sure to check out our list of trusted resources.**