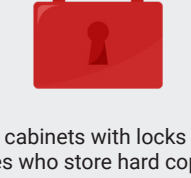
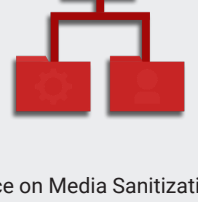
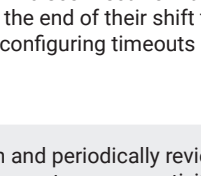
INFINIT-O is HIPAA Compliant

Your company and patient data are safe with us

INFINIT-O
Endless Opportunities

HIPAA Security Checklist	Compliance	Monitoring
Ensure proper configuration of devices that access company and client data (i.e., are encrypted, with password, firewall, and antivirus protection)	Computers & laptops were provided to team members that are set-up with standard security requirements: · Active Directory Membership · Full Disk Encryption · Firewall · Antivirus/Antimalware Software · Two-factor authentication	Installing remote management software for Infinit-O IT team to monitor and deploy security patches and update firewall configurations regularly
 Secure home networks (i.e routers, dongle, etc.) and working area	· Launched mandatory security awareness courses for all team members · Information drive for security-related resource material for latest trends & updates · Submission of IT & security checklist to team members to meet the remote work set up technical requirements · Teleworking and Mobile Device Policy in place wherein team members who must connect via Wi-Fi will utilize WPA2 standard (as minimum) and adhering to Infinit-O password provisions	· Automated completion reports notification email to managers for compliance monitoring · Quarterly Infosec & Data Privacy awareness quiz for all team members
Encrypt password-protect on devices employees use to access PHI remotely	Supplying company computers and laptops with full disk encryption enabled by native Microsoft Bitlocker or IOS Filevault	Installation of remote management software which allows Infinit-O to monitor and audit full disk encryption status
 Configuration of devices for home use	Automatically filtering devices prior to connecting to VPN servers and before granting access to Infinit-O's network. Checking the following presense: **A.** OS version and security patch details **B.** Company antivirus software with latest definition and most recent scan requirement **C.** Firewall will be enabled **D.** Full disk encryption	· Firewall and VPN systems automatically allows connection if devices pass the security requirement and block it if otherwise · An alert notification will be sent to Infinit-O's security team if an attempt to connect is made but not passing the authentication requirements for further investigation
 Encryption of PHI before transmission	· Method of transmission is agreed upon with the clients/vendors beforehand. Normally transmitted via our servers or cloud-based file sharing with end-to-end encryption protocols. · EHPI files are encrypted and password protected prior to sending to secured channels.	Email servers and cloud-based sharing are regularly audited by 3rd party firms to ensure HIPAA compliance
Develop policies and procedures prohibiting employees from allowing friends and family from using devices that contain PHI	Adhering to Infinit-O Teleworking and Mobile Device Policy "Users conducting teleworking/mobile working will not allow or give permission for unauthorized users (including family and friends) to use that PC/ mobile device."	· Team members are required to read and sign off our Acceptable Usage policies · Automatic locked out system for devices inactive for a 8 minutes
Signing of Confidentiality Agreement for employees	Infinit-O team members are required to sign an NDA & other network acceptable usage policies as part of the contract	Regular exams are conducted to monitor security awareness level
 Bring Your Own Device (BYOD) Agreement are signed with clear usage rules	Excerpt from Remote Working Agreement: The following software will be installed to your personal equipment to use it for work purposes. · Symantec Antivirus · Global Protect VPN · Managed Zoom Account · Managed Engine Desktop Central (Remote Desktop Management Software) · Chrome Browser and work related extensions	Installation of remote management software which allows Infinit-O to monitor and audit full disk encryption status
 Provide file cabinets with locks or safes for employees who store hard copy (paper) PHI in their home offices	With the remote set up, no lockers are provided but printing and USB access are disabled on all remote computers	Printing and USB/device connections are controlled through Windows Active directory Group Polices and Symantec endpoint protection software Email notifications are sent out in case team members plug in unauthorized devices (e.g. USB disk, printers) to IT security team for further investigation and proper sanctions
Providing HIPAA-compliant shredders for remote workers for proper disposal of PHI hard copies	Paper shredders are not provided but the Control of Records Policy outlines how to protect PHI hard copies	
 Adherence on Media Sanitization Policy	IO's Control of Records Policy clause: "Media containing information, regardless of classification, must be disposed of in a secure and reliable way. (i.e., shredding, destruction)" IO's IT Disposal policy states: "All non-operational Disk/Removable media will be physically destroyed while all Operational Disk/Removable media drives must be erased via military grade multiple overwriting process application or through use of disk nuking software"	Asset disposal request and media sanitazion reports are submitted accordingly
Employees will disconnect from the company network at the end of their shift through IT configuring timeouts	End users are disconnected automatically from corporate VPN networks after 15 minutes of inactivity. Reauthentication is needed to reconnect to the VPN.	
Maintain and periodically review logs of remote access activity	Firewall/VPN systems automatically collects and logs remote connections and network activities.	Regular review of access and VPN logs by the IT security team