|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| COMPUTER DATA ACCESS AND SECURITY | | | | NO. | |
| Administrator will determine the Protected Health Information (PHI) stored electronically an employee needs to access, and at what level, to perform their job functions.  Users will sign on to software applications containing PHI with a unique identification (ID) and password. Passwords are changed on a regular basis or as needed.  A master list of IDs and passwords will be maintained by the Information Technology (IT) Coordinator, to which the Administrator and/or their designee will have access.  User activity will be monitored, recorded and examined by the IT Coordinator and/or the Administrator/designee. Inappropriate activities will be reported to Administration.  The Personnel department or Office Manager will notify the IT Coordinator and/or the Administrator/designee when an employee leaves the organization or changes positions to initiate termination of computer access as of the last work date. A post-employment checklist (attached) will be completed for quality assurance purposes. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| E-MAIL ACCESS AND SECURITY | | | | NO. | |
| Administrator will determine if an employee needs access to e-mail to perform their job functions.  E-mail users will have a unique Identification (ID) and password.  A master list of IDs and passwords will be maintained by the Information Technology (IT) Coordinator, to which the Administrator and/or their designee will have access.  Confidentiality notices will automatically accompany e-mails containing protected health information (PHI).  Users should disable the preview pane option in their email application.  Users should avoid opening emails from unknown senders. These should be deleted without opening or previewing.  User activity will be monitored, recorded and examined by the IT Coordinator and/or the Administrator/designee. Inappropriate activities will be reported to Administration.  The Personnel department or Office Manager will notify the IT Coordinator and/or the Administrator/designee when an employee leaves the organization or changes positions to initiate termination of e-mail access as of the last work date. A post-employment checklist will be completed for quality assurance purposes. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VOICEMAIL ACCESS AND SECURITY | | | | NO. | |
| Administrator will determine if an employee needs access to voicemail to perform their job functions.  Voicemail users will have a unique identification (ID) and password.  A master list of IDs and passwords will be maintained by the Information Technology (IT) Coordinator, to which the Administrator and/or their designee will have access.  The Personnel department or Office Manager will notify the IT Coordinator and/or the Administrator/designee when an employee leaves the organization or changes positions to initiate termination of voicemail access as of the last work date. A post-employment checklist will be completed for quality assurance purposes. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| LAN SERVER ACCESS AND SECURITY | | | | NO. | |
| A server storing Protected Health Information (PHI) will be located in a physically secure area.  A server storing PHI will be backed up in its entirety nightly, Monday through Friday, by the Information Technology (IT) Coordinator and/or the Administrator’s designee. Back up tapes will be stored in a physically secure area off site. Access will be limited to the IT Coordinator and/or the Administrator/designee.  A server storing PHI will have virus protection software installed, maintained and updated on a regular basis by the IT Coordinator and/or the Administrator/designee.  The IT Coordinator and/or the Administrator/designee will have access to perform server configuration. Passwords are changed on a regular basis or as needed.  A master list of identifications (IDs) and passwords will be maintained by the IT Coordinator to which the Administrator and/or their designee will have access.  User activity will be monitored, recorded and examined by the IT Coordinator and/or the Administrator/designee. Inappropriate activities will be reported to Administration.  The Personnel department or Office Manager will notify the IT Coordinator and/or the Administrator/designee when an employee leaves the organization or changes positions to initiate termination of server access as of the last work date. A post-employment checklist will be completed for quality assurance purposes. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| WORKSTATION ACCESS AND SECURITY | | | | NO. | |
| Where feasible, workstations/terminals will be positioned or shielded to prevent more than incidental observation of work product.  Workstations that connect to the server will have virus protection software installed, maintained and updated on a regular basis by the Information Technology (IT) Coordinator and/or the Administrator/designee.  Users will sign on to their workstation with user identification (ID) and password.  A password-protected screensaver will activate automatically on workstations after a period of inactivity.  Passwords are changed on a regular basis or as needed. Users may not automate their password entry.  A master list of IDs and passwords will be maintained by the IT Coordinator to which the Administrator and/or their designee will have access.  Users will power off their workstations at the end of their day.  Users will secure media that contains Protected Health Information (PHI) in a locked desk, cabinet or room.  Software will be loaded on workstations by the IT Coordinator and/or the Administrator/designee.  Equipment will be connected to a workstation by the IT Coordinator and/or the Administrator/designee.  User activity will be monitored, recorded and examined by the IT Coordinator and/or the Administrator/designee. Inappropriate activities will be reported to Administration.  Administration reserves the right to conduct periodic spot audits of workstations and to remove applications or data which has been placed there inappropriately.  The Personnel department or Office Manager will notify the IT Coordinator and/or the Administrator/designee when an employee leaves the organization or changes positions to initiate termination of workstation access as of the last work date. A post-employment checklist will be completed for quality assurance purposes. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DISCARDING / REPLACING ELECTRONIC MEDIA | | | | NO. | |
| Electronic media discarded or replaced (including hard drives in workstations) will be overwritten or irrecoverably destroyed to ensure proper erasure of Protected Health Information (PHI). The IT Coordinator and/or the Administrator’s designee will ensure that media has been thoroughly cleansed of PHI before the media is surplussed or disposed of. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PORTABLE ELECTRONIC EQUIPMENT | | | | NO. | |
| A master list of users assigned portable electronic equipment will be maintained by the Information Technology (IT) Coordinator, to which the Administrator and/or their designee will have access.  User activity will be monitored by the IT Coordinator and/or the Administrator/designee. Inappropriate activities will be reported to Administration.  The Personnel department or Office Manager will notify the IT Coordinator and/or the Administrator’s designee when an employee leaves the organization or changes positions to initiate the return of assigned portable electronic equipment as of the last work date, and verified by the post-employment checklist. | | | | | |
| Approved: | Effective Date: | Revision Date:  3/17 | Change No.: | | Page:  1 of 1 |