|  |  |
| --- | --- |
|  SAFEGUARDS FOR USE OF ELECTRONIC MAIL  | NO.  |
| It is the policy of the organization to observe the following practices for its employees who are granted access to the electronic mail system:1. Do not forward any resident-identifiable information to a third party without the resident’s authorization, in writing (unless stipulated in the privacy notice).
2. Even if the resident or resident’s family requests that information be e-mailed, be sure that they know the possible risks of sending personal information. Don’t assume everyone knows how e-mail works. Inform them of the possibilities of misdirected or intercepted personal information getting into unauthorized hands.
3. There is some information that should never be e-mailed or faxed. Results of HIV tests, for example, should never be communicated via fax or e-mail.
4. If you receive e-mails from residents’ families that may contain sensitive materials, be sure to notify them when your e-mail is down. Keep a log of which residents’ families use e-mail to ensure proper notification.
5. ALWAYS have a confidentiality notice with a disclaimer on a cover sheet or at the end of e-mail.
6. Be sure you are sending your e-mail to the correct address. DOUBLE CHECK before sending! If you haven’t contacted a party for a while, confirm that the e-mail address is still the same. Keep your e-mail address/log book up-to-date.
7. Avoid location of personal computers with e-mail accounts in an area where e-mail could be viewed or accessed by unauthorized personnel.
8. Security e-mail accounts are maintained with password protection. Passwords will be deleted from the systems as part of the post-employment process.
9. Print out all e-mails and file the hard copies in the resident’s medical record.
10. Only those staff members authorized are allowed to e-mail confidential information; those who are permitted to do so must be knowledgeable about related policies and are properly trained.

  |
| Approved: | Effective Date: |  | Change No.: | Page: 1 of 1 |