VERMONT

Agency of Human Services
HIPAA Guidance Working at Remote or Temporary Locations and Health Information

If you are authorized to work at a remote or temporary location and your job requires that you access, create, use and/or disclose health information, you must:

- keep all health information **private and secure**, and
- only access, create, use and/or disclose the **minimum necessary** amount of health information.

Follow these rules for the road for working at remote or temporary locations:

1. You should transport health information, in paper or electronic form, in your car only when it is absolutely necessary and only after consulting with your supervisor. If you must transport health information in your car, you must take all possible steps to ensure that the health information is not left unattended in your car. If you must leave it in your car, you must make sure your car is locked and the information is hidden from plain view.

2. You must keep electronic and paper health information in a secure place. You must make sure that it can not be accessed by individuals who do not have the authority to do so. You must not leave health information in plain view or in common areas.

3. If as part of your job you make phone calls in which you discuss health information, you must be discreet. If you have a door to your work space, be certain to close it. If you share your work space, speak softly if possible so that others do not overhear your conversation.

4. You must follow the rules for the road for laptop/portable devices such as usb flashdrives, IPods, CDs, DVDs, diskettes, and PDAs found in the **AHS Laptop/Portable Device Security Information Sheet** located on the AHS Intranet site at http://intra.ahs.state.vt.us/centralsupport/hipaa/hipaadocs/ahs_laptopsecurityinfo.pdf.

5. You should consult with your supervisor and your department's IT staff as to the security of the computer system that you are using. At a minimum, any computer being used to access AHS information systems should have current versions of antivirus and antispyware software which are set to update automatically daily. In addition, the computer should be set to daily autoupdate Windows. At no time should you use personal email to transmit any work information. You must use the provided Outlook or secure Outlook Web Access to ensure email confidentiality. When using Outlook Web Access do not download and save attachments containing confidential information onto your local system.

6. If you believe that health information has been lost, stolen, or accessed by inappropriate persons, you should contact your supervisor and the AHS Privacy Officer, Martha Csala, at 802-241-2513 or martha.csala@ahs.state.vt.us. If the health information is in electronic form, you should immediately contact the AHS Security Officer, Darin Prail, at 802-241-1130 or darin.prail@ahs.state.vt.us. You should also work with your supervisor to complete and submit an **AHS Privacy and Security Incident Report form**, which can be found at http://intra.ahs.state.vt.us/centralsupport/hipaa/hipaadocs/ahs_hipaa_privacysecurityincidentreportform.dot.