VAN BUREN COMMUNITY MENTAL HEALTH AUTHORITY
POLICIES & PROCEDURES

Title: Electronic Communications
Number: I.01.08
Originated: 11/04/97
Approved By: Executive Team
Revised: 9/17/02, 6/20/05, 10/21/09, 11/11/15

PURPOSE:

This procedure has been established with regard to access and disclosure of all electronic communications, including but not limited to, internet or intranet communications, and voice and fax messages created, sent or received by employees using Van Buren Community Mental Health's (VBCMH) electronic communications systems. All communications systems should be used for business relating to the operations of VBCMH and for no other purposes.

VBCMH's electronic communication systems must generally be used only for business activities. Incidental personal use is permissible so long as:

a. It does not consume more than a trivial amount of resources
b. It does not interfere with staff productivity.
c. It does not preempt any business activity.

Use of VBCMH's electronic communication systems for malicious or illegal purposes or commercial activities outside the business objectives of VBCMH is strictly prohibited.

There should be no expectation of staff privacy for any materials stored on or transmitted through the electronic communications systems as all transmissions are the sole property of VBCMHA and may be subject to disclosure under the Freedom of Information Act.

DEFINITIONS:

Electronic Communication System: Includes but not limited to, computer systems, E-mail, voice mail, telephones, fax, Internet, and Intranet owned, leased or operated by VBCMH.

E-Mail: Electronic communication via the computer system.

Voice Mail: Telephone answering system.

Fax: Facsimile transmissions.

IT: Information Technology.

Freedom of Information Act (FOIA): a Public Act that requires a public body to provide access to all of its "public records" except those specifically exempt from disclosure. "Public record" is a writing prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function, from the time it is created. VBCMH may be required to turn over electronic communications to other governmental authorities or others in the course of an investigation or litigation.

Health Insurance Portability & Accountability Act (HIPAA): A Public Act, adopted in 1996, which calls for standardization of electronic patient health, administrative and financial data, unique health identifiers for individuals, employers, health plans and health care providers, and security

standards protecting the confidentiality and integrity of "individually identifiable health information," past, present or future.

DIRECTIVE:

Employees are strictly prohibited from creating and sending electronic communications that are harassing, intimidating, discriminatory, rude, vulgar, or offensive in any way. The use of electronic communication systems for any of these purposes may result in discipline of the employee, up to and including termination of employment.

Employees will not forward chain letters, urban legends (fact or fiction), or other offensive, time consuming, or non-business related e-mails to individuals inside or outside the VBCMH network.

While confidentiality is encouraged and should be respected, electronic communications are not private and confidentiality is not guaranteed. Van Buren Community Mental Health reserves the right to monitor all electronic communications of all users of the system, and to use the information discovered in those messages for any and all purposes permitted.

PROCEDURES:

These procedures shall serve as a guideline to assure appropriate use of the electronic communications systems within the Agency.

1. The level at which staff are authorized to access the electronic communication system will be at the discretion of the Division Manager. Staff requesting a higher level of access, including internet access, must submit such request in writing to their Supervisor and Division Manager for approval. The Human Resources office will coordinate access with IT, upon request from the Division Manager.

2. All passwords are designated by the user and should not be shared. If, for any reason a new password is needed, contact IT to have the password reset. Once reset, the user will be required to change the password on the next logon. Passwords are confidential for security purposes and should not be known to anyone except the user.

3. The electronic communication system hardware is VBCMH property. Additionally, all messages composed, sent, or received on the electronic communication system are and remain the property of the agency. They are not the private property of any employee.

4. The electronic communication system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive, are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.

CONDITIONS AND LIMITATIONS:

1. The use of the agency electronic communication system was designed for conducting agency business. It is not intended for personal business. Employees will not forward chain letters, urban legends (fact or fiction), or other offensive, time consuming, or non-business related e-mails to individuals inside or outside the VBCMH network.

2. Employees will not create or forward mass personal e-mails to persons inside or outside the agency. E-mail distribution groups such as, VBCMH, HSB, CSDD, SHOP, HFRC, HOPE, MTI, etc. were specifically created for the sole purpose of conducting agency business and may not be used for non-business related purposes.

3. The electronic communication system may not be used to solicit or proselytize for commercial ventures, religious or political causes, or outside organizations.

4. The electronic communication system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

5. VBCMH reserves, and may exercise, the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic communication system for any purpose.

6. Notwithstanding the Agency's right to retrieve and read any electronic communication messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any electronic communications that are not specifically sent to them.

7. In accordance with HIPAA regulations, special consideration must be taken when handling customer information across electronic communications media. All customer information is considered Protected Health Information (PHI), whether it is electronic (ePHI) or paper. E-mails containing customer protected health information may only be sent, forwarded, or replied to within the VBCMH network, including those individuals whose e-mail addresses end with "@vbcmh.com". It is imperative that you do not send, reply to, or forward information to individuals outside VBCMH's protected network that contains any customer's protected health information without first encrypting the message. The encrypt button is found near the Send button.

8. Employees shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Employees shall not gain, or attempt to gain, unauthorized access to other users' computers or the VBCMH computer system. Employees shall not attempt to gain access to another employee's messages without the latter's permission.

9. Any violation of this procedure will be subject to discipline, up to and including termination of employment.

10. Violations of this procedure that do not involve a customer's protected health information should be reported to the supervisor or the Human Resources Office for investigation. Violations involving a customer's protected health information should be immediately reported to the Corporate Compliance Officer.