computer's hard drive (C: Drive) or any other network drive than the one designated as HIPAA-Data. This ensures that the appropriate protections are in place for sensitive protected health information.

- **Strong Passwords** - There are programs that can crack weak passwords, for example, dictionary words and common names. That's why passwords should contain upper and lower case letters, as well as numbers and special characters.
- **Viruses** - Many viruses are spread by inserting copies of themselves as attachments to e-mails that are then sent to the victim's address list with the appearance of coming from friends or associates. If an e-mail attachment looks suspicious, do not open it.
- **Web Based E-Mail** - OMH employees can no longer access web based e-mail accounts over the Internet. This includes hotmail, yahoo mail and others.

Violations

OMH will review alleged violations on a case by case basis. Violations may result in administrative action, which may include disciplinary action as appropriate.

Keep in Mind

If you have questions about OMH Information Security, you may refer back to the OMH Information Security Policy, consult your OMH Information Security Learning Guide, ask your supervisor, facility Information Security Liaison (ISL), or a staff member from your education and training department for assistance.

Remember...Information Security is everyone's responsibility.

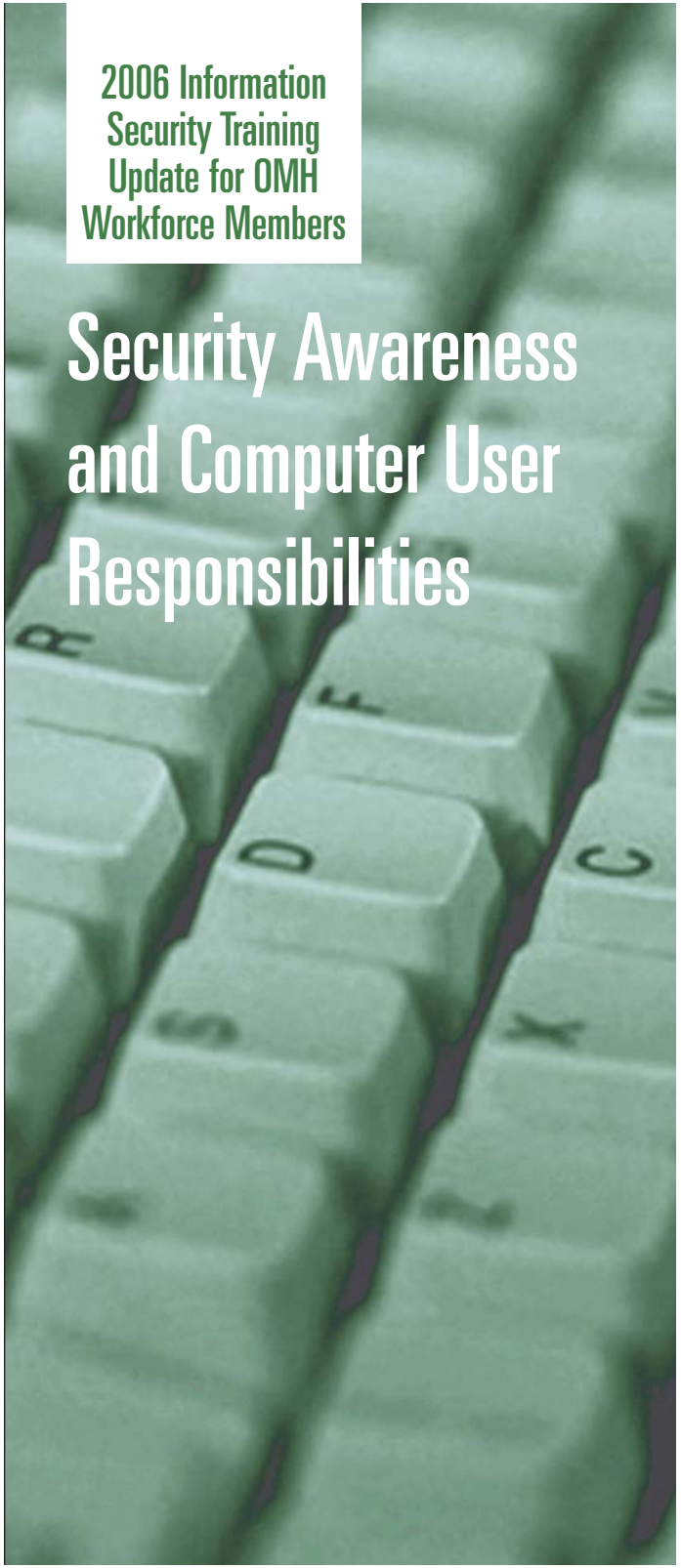
Thank you!

Prepared by the OMH Bureau of Education and Workforce Development in conjunction with the OMH Information Security Unit

New York State
George E. Pataki, Governor

Office of Mental Health
Sharon E. Carpinello, RN, PhD, Commissioner

November 2006



2006 Information Security Training Update for OMH Workforce Members

Security Awareness and Computer User Responsibilities

Please note:

Every member of the OMH workforce, regardless of job title or function, is mandated to read this brochure and document receipt as instructed by their Education and Training Office. If you have questions, please direct them to your Education and Training Office.

Why am I receiving this brochure?

The reasons you are receiving this brochure are to update you regarding your responsibilities related to computer usage and to heighten your awareness about Information Security.

As a member of the OMH workforce, you have received training in OMH Information Security and should already know your responsibilities related to computer usage.

If you need a refresher, please review your copies of the 2005 OMH Information Security Training Learning Guide or the 2003 OMH HIPAA Privacy Training Learning Guide. These guides can be accessed by going to the following websites:

http://inside.omh.state.ny.us/cism/security/training/learningguide.pdf

http://www.omh.state.ny.us/omhweb/hipaa/training/learningguide.htm

OMH Information Security

Remember...

- **Never** install any non-OMH hardware on the network.
- **Never** install any non-OMH software on your computer or laptop.
- **Never** download or distribute illegal or inappropriate material.
- **Never** leave Protected Health Information (PHI) or other confidential information on you computer screen when you leave your workstation. Make sure you log-off or lock your computer when you are away from it.
- **Never** share your password or token with anyone and do not write down passwords or token pin numbers.

Some key terms and definitions that you should know:

- **Phishing** - E-mails sent to users with the purpose of tricking them to sign onto a spoofed website to enter personal or financial information. Banks are often targets of phishing scams. It is important not to click on links to websites sent in e-mails. Links can easily send you to a website that is not the actual organization's site, even though it may appear to be.
- **Social Engineering** - A method used in the attempt to gain unauthorized access to information that involves and relies upon misrepresentation or "tricking" someone into disclosing information. Just like you would never offer up your bank pin number to a stranger, you should never offer passwords or confidential OMH information over the phone, via e-mail, or in person. The OMH Helpdesk will never call or e-mail unsolicited, to ask for your user-IDs or passwords.
- **SPAM** - Unwanted e-mail communication sent in mass quantities. Some SPAM is harmless, although annoying (like commercial advertising), while other SPAM is more malicious in nature. Please be aware that giving out your e-mail address increases the amount of SPAM you receive.
- **Spyware** - Software that collects information about the websites that a user visits for marketing purposes or possibly to gather personal information to use maliciously. It is often considered an invasion of privacy. Spyware can be downloaded onto your computer simply by visiting a website or can be included in free or commercial downloads.
- **Store Protected Health Information (PHI) in HIPAA Drive** - It is imperative that PHI is stored in the designated HIPAA Drive and NOT on your