

eCHN Safe Computing Practices

It is important that you take steps to protect your information on your personal computer. The **electronic Child Health Network (eCHN)** is a protected environment which meets the highest Internet security standards.

While we take strong measures to ensure the security and confidentiality of patient information, it is extremely important that you also take precautions to ensure that patient information remains safe and secure when accessing the information from your computer.

We advise all health care practitioners to read about these topics and follow the recommended safe computing practices:

- [Protect Your Privacy](#)
- [Use Anti-Virus Software](#)
- [Protect Your Internet Connection](#)
- [Wireless security](#)
- [Use Supported Browsers](#)
- [Password Guideline](#)

Last Revised: August 2008

Protect Your Privacy

- Always type in the website address or use your bookmarks to access eCHN
- Do not leave your computer unattended while logged on to eCHN.
- Always log off when you are finished your eCHN session.
- Clear your browser's cache after each eCHN session. Each time you access the Internet, your browser automatically saves a copy of the web pages you've visited. Diligently clearing your browser's cache after each session is an important step in safeguarding the personal health information of your patients. See the section "How and Why to Clear your Cache" at

Microsoft - How to clear your cache -

<http://www.microsoft.com/windows/ie/ie6/using/howto/customizing/clearcache.msp>

- Know that eCHN will never present you with unexpected web pages or send you unsolicited emails asking for your user name and password, etc.
- Do not respond to unsolicited emails or websites that request personal information. eCHN will never ask you to validate or restore your account access through unsolicited email.

- Protect your user name and password. Always remember to keep your eCHN user name and password secret. Do not divulge your password to anyone. If you suspect your password has been compromised, please change your password immediately or call the eCHN helpdesk at 416.813.7998.
- Report any suspicious requests to eCHN immediately - privacy inquiry number 416.813.8420 or eCHN Help Desk at 416.813.7998.
- Use a password that is difficult to guess by using a combination of letters and numbers.
- Never send personal health information via email or Instant Messaging.
- Avoid using software or browser settings that records your passwords so that you don't need to enter them the next time you access a website from the same computer. This type of software could give other users of your computer access to your account.
- Avoid using the Internet in public places (such as Internet cafes, libraries, etc.) to access your HiNet account. These have been known to have software that records your personal information, which can be used fraudulently.
- Use caution before answering online and email requests for your personal information.

Use Anti-Virus Software

Whenever you use your personal computer and the Internet, there is a potential risk of contracting a computer virus or the possibility of infiltration by intrusion software commonly known as "Trojan Horses". Computer viruses can modify programs, delete files and erase the contents of hard drives. "Trojan Horses" can have similar effects and may be able to capture keystrokes, including passwords or other secret information. Spyware and other deceptive software can also conduct certain activities on your computer without your knowledge or consent with possibility of disclosing the personal health information to the originator of the Spyware. The potential consequences of any of these threats could include damage to your personal computer, compromise the security of patient information and the inability to use eCHN. For these reasons, eCHN advises all users to follow these practices:

- Install and frequently update a proven anti-virus product, such as *Norton Internet Security 2007*, *McAfee VirusScan Plus 2007* or *Trend Micro AntiVirus plus AntiSpyware 2007*. Most popular anti-virus products include some spyware scanning capabilities.
- Only accept or download software from a source that you believe to be trusted.
- Never accept files or attachments when accessing websites, newsgroups and chat rooms unless you are sure of their authenticity.
- Ensure you are using legally licensed operating system software.

Protect Your Internet Connection

There are additional vulnerabilities associated with having a computer directly connected to the Internet for an extended period of time. These vulnerabilities apply to all internet users but it is especially important for internet users with cable modem or digital subscriber line (DSL) Internet access. These methods of connection do not require 'dialing' to be connected to the Internet and thus are sometimes described as 'always on' connections. Unfortunately, as long as the computer remains 'on' and connected to the Internet, malicious parties have a continuous window of opportunity for attacks on the user's

personal computer. If you use a cable modem or DSL connection for Internet access, you can limit this security risk by disconnecting from the Internet when your session is complete, or by turning off the cable or DSL modem. However, if you want to continue to take advantage of the 'always on' feature of cable and DSL connections or if you run extended dial-up sessions on the Internet, we recommend the following security measures:

- **Disable File Sharing on Your Personal Computer:** File sharing is a feature of Windows that allows other computers to access your personal computer, even via the Internet. Microsoft has provided instructions on how to disable file sharing in Windows Help (Click Start, Help, then choose the 'Index' tab and type "file sharing, disabling"). Our recommendation is to disable file sharing. However, if you choose to retain this option for your particular environment, exercise due care and apply appropriate security measures.
- **Install a Personal Firewall:** Install and frequently update a proven personal firewall product, such as Zone Alarm, Kerio, Black Ice or Windows XP Firewall, which can be configured to prevent unauthorized access to your personal computer. It is important to keep the firewall product up-to-date.
- **Get Computer Security Updates:** Ensure that you are using a legally licensed operating system. You may be able to improve the security of your system by getting updates to help correct issues that may make your computer vulnerable to viruses, worms and other exploits. As such, you should diligently apply security patches as they become available or enable automatic updates as part of operating system options, where applicable.

Wireless security

Wireless networks are more and more common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed for the buyer. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into non-wireless networks. Because of security risks as listed below eCHN does not encourage its users to access HiNet through wireless network. Although wireless network is not encouraged for HiNet access if implemented it is recommended that minimum security steps has to be followed as outlined in the [Steps in Securing a Wireless Network](#)

Security Risks

Wireless being used to crack into non-wireless networks

Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A cracker could sit out in the parking lot and break in through the wireless card on a laptop and gain access to the wired network. If no security measures are implemented at these access points, it is no different from providing a patch cable out the back door for crackers to plug into whenever they wish.

Types of unauthorized access to company networks

Accidental Association - This is when a user turns on their computer and it latches on to a wireless access point from a neighboring company's overlapping network. The user may not even know that this has occurred. However, this is a security breach in that proprietary company information is exposed and

now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

Malicious Association – are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans.

Identity Theft (MAC Spoofing) - occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges.

Man-In-The-Middle Attacks - This attack revolves around the attacker enticing computers to log into his/her computer which is set up as a soft AP (Access Point). Once this is done, the cracker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent cracking computer to the real network. The cracker can then sniff the traffic for user names, passwords, credit card numbers...etc.

Denial of Service - occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users not to be able to get on the network and may even cause the network to crash.

Steps in Securing a Wireless Network

The following are some basic steps that are recommended to be taken to secure a wireless network; in order of importance:

1. Turn on encryption. WPA2 encryption should be used if possible. WPA encryption is the next best alternative, and WEP is better than nothing.
2. Change the default password needed to access a wireless device — Default passwords are set by the manufacturer and are known by crackers. By changing the password you can prevent crackers from accessing and changing your network settings.
3. Change the default SSID, or network name — Crackers know the default names of the different brands of equipment, and use of a default name suggests that the network has not been secured. Change it to something that will make it easier for users to find the correct network. You may wish to use a name that will not be associated with the owner in order to avoid being specifically targeted.
4. Disable file and print sharing if it is not needed — this can limit a cracker's ability to steal data or commandeer resources in the event that they get past the encryption.
5. Access points should be arranged to provide radio coverage only to the desired area if possible. Any wireless signal that spills outside of the desired area could provide an opportunity for a cracker to access the network without entering the premises. Directional antennas should be used, if possible, at the perimeter directing their broadcasting inward. Some access points allow the signal strength to be reduced in order to minimise such signal leakage.
6. Divide the wired and wireless portions of the network into different segments, with a firewall in between. This can prevent a cracker from accessing a wired network by breaking into the wireless network.

7. Disabling the SSID broadcast option — Theoretically, hiding the SSID will prevent unauthorized users from finding the network. In fact, while it will prevent opportunistic users from finding the network, any serious cracker can simply scan your other network traffic to find the SSID. It will also make it harder for legitimate users to connect to the network, since they must know the SSID in advance and type it in to their equipment. Hiding the SSID will not prevent anyone from reading the data that is transmitted, only encryption will do that.
8. Enabling MAC address filtering — MAC address filtering will prevent casual users from connecting to your network by maintaining a list of MAC addresses that are allowed access, (or not) but a serious cracker will simply scan your network traffic to find a MAC address that is allowed access, then change their equipment to use that address. Any new equipment will require another MAC address to be added to the list before it can be connected. Again, enabling MAC address filtering will not prevent anyone from reading the data that is transmitted without encryption.
9. Wireless router firmware has to be updated on regular basis.

Additional Information

- "Best Practices for Rogue Wireless LAN Detection" A white paper by AirDefense, Inc. © 2003 AirDefense, Inc. From <http://www.airdefense.net>
- "Wireless LAN Security: What Hackers Know That You Don't" A white paper by AirDefense, Inc. © 2002-2005 AirDefense, Inc. From <http://www.airdefense.net>
- "Layered Approach to Wireless Network Security and Management" A white paper by AirDefense, Inc. © 2002-2005 AirDefense, Inc. From <http://www.airdefense.net>
- "Wireless Security — Four Steps you need to Take" <http://www.linksys.com/edu/page10.asp>
- Linksys's "Educate Me/Wireless Security—Wi-Fi Protected Access™ (WPA) Security" at <http://www.linksys.com/edu/wpa.asp>

Use Supported Browsers

Encryption is the process of protecting information as the information moves from one computer system to another computer system in such a way that the information is unreadable to everyone except the parties involved. The stronger the level of encryption used by your web browser, the more difficult it is for unauthorized parties to break the encryption and decipher the message in transit. The eCHN application HiNet (Health Information Network) is fully tested before supporting new browser versions. When accessing eCHN's HiNet, you are required to use one of our recommended browsers with 128-bit encryption. This process will be explained during the HiNet installation process. Please contact eCHN Help Desk at 416 813 7998 for more information.

Password Guideline

Passwords are an important aspect of computer security. They are the front line of protection for user accounts and some of the best practices for protecting password are:

- Password must be changed at least every three (3) months.
- Password must not be inserted into email messages or other forms of electronic communication.
- For optimum security, don't write your password down. Don't post it anywhere around your desk.
- Don't type your password while anyone is watching.
- Do not let anyone else know or use your password;
- Don't reveal a password on questionnaires or security forms
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

How to create a strong password

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#%&*()_+|~-=\`{}[]:";'<>?.,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- One of the easiest to remember and hardest to crack password methods is the pseudo-random password. The actual password is generated from an easy to remember phrase that is important to the user. This phrase can be the words from a favourite book, words from a favourite song, or something similar. The key to a successful password is to create a phrase that is easy to remember, but no one else will be able to guess.
 - **personal phrase:** "Four score and seven years ago our fathers brought..."
password: 4scanse...
method: Chose first two letters from each word until a total of eight characters resulted.
 - **personal phrase:** "It was a dark and stormy night...".
password: iWadasn...
method: Chose first letter from each word, followed by ellipses.
 - **personal phrase:** My Brother's Birthday Is april(4) Twenty Second Nineteen Sixty three(3)
password: mbbi4t\$ns6
method: Chose first letter from most words, with addition of special character.

NOTE: Do not use either of these examples as passwords!

Avoid a weak password

When creating passwords, the following should be avoided:

- Easy to guess passwords such as "*****" or "password"
- Names of family, pets, friends, co-workers, fantasy characters, etc
- Computer terms and names, commands, sites, companies, hardware, software
- String of numbers or characters, like 1234, abcde, aaabbb, qwerty, zyxwvuts, 123321, etc
- The hostname of your computer
- Birthdays and other personal information such as addresses and phone numbers, license plate number, etc
- A username in any form (as is, capitalized, doubled, etc.)
- A word in the English dictionary or in a foreign dictionary
- Place names or any proper nouns
- Passwords of all the same letter
- Any of the above spelled backwards
- Any of the above followed or preceded by a single digit (e.g., secret1, 1secret)

Additional Information

There is a number of web sites that provide more information on Internet Security and Safe Computing. The following references are included for your information:

CERT – Home computer security <http://www.cert.org/homeusers/HomeComputerSecurity/>

While eCHN believes these safe computing practices and included links provide reasonable protection, eCHN makes no representation or warranty as to their intended use.