INFORMATION SECURITY BASICS
University of Miami Ethics Programs

WHY WORRY ABOUT THIS?

Without good information security, an organization's entire business operation is at risk. So is its customers' privacy. That's particularly critical with sensitive personal health information – and it's why information security measures are required by federal and state law, institutional certification organizations' requirements, business common sense and the principles of medical ethics.

A security system is only as good as its weakest link – so every dimension of security is important. Many of the rules listed here may seem obvious, but it is common to find violations of them every day. In many cases a security problem can be fixed with a simple change in your own behavior, or a gentle reminder to a colleague. But if you find a problem that you cannot correct, or have any questions or concerns, contact a supervisor, your organization's privacy office or its information security office. *Don't assume that someone else will "fix it" – that's what turns small problems into big ones.*

If you're not sure about something, ask a colleague, a supervisor or contact your organization's privacy office or information security office. Some mistakes cannot be undone.

PHYSICAL SECURITY

Controlling physical access to an organization's facilities is one of the most important elements of security:

- Locks, alarm systems and other devices should be installed – and in operation – to keep an area appropriately secure when not open for business.
- When open for business, unattended areas should still be kept secure with locks and other devices whenever possible. (If a door to a restricted area can't be locked, it should at least be closed.)
- Physical access to sensitive office equipment should be controlled – that includes computers, printers, photocopiers, fax machines and old-fashioned file cabinets full of paper records.
- Visitors should be appropriately monitored and escorted, to ensure that they do not access restricted areas. Unidentified persons in restricted areas should be (politely) challenged.
- If you are given keys, tokens, ID badges or anything else that allows physical access, make sure you keep them secure. *File a security report immediately about anything that is lost or stolen.*

ORAL COMMUNICATIONS (TALKING)

Everyone knows how to talk. But we all know that not everyone knows how to do it in a secure way:

- Conversations involving sensitive information should not occur where they can easily be overheard. (Notice how loudly many people talk in public places?)
- Names or other information that could identify individuals should be avoided in conversations whenever possible, just in case the conversation is overheard.

- “Quiet areas" (away from public areas) should be used for sensitive information exchange whenever possible.

- When it cannot be avoided, sensitive discussions that occur in public areas should be conducted as quietly as possible.

- Only a patient's name should be called out in waiting rooms or used on intercom/paging systems. And avoid even that when you can.

INFORMATION ON PAPER

It’s the electronic age, but paper is still everywhere. So protecting it is still important:

- Sensitive documents should not be left on unattended computer printers, photocopiers, or fax machines (and those devices should be in secure locations).

- Sensitive documents should never be left in plain view in areas where visitors are present (for example, if records must be left on a door rack, identifying information must be obscured).

- If sensitive documents must be left in an area where visitors may be present, they should be face down or otherwise concealed.

- Sign-in sheets should contain only limited information (ideally, only the patient's name). Patient schedules should not left be in public areas or where they can be easily viewed by non-staff.

- Sensitive documents that are no longer needed should be shredded immediately – or placed in an appropriate container for secure disposal in the near future.

TELEPHONE USE

Sometimes it’s the most familiar devices that present the greatest security risks:

- Telephone conversations involving sensitive information should be conducted where they cannot be overheard, if at all possible. That especially includes conversations on cell phones. (Ever notice how loudly many people talk on their cell phones?)

- When discussing confidential information with a patient, or about a patient to a third party, the other person's identity should always confirmed before proceeding.

- Only names and callback numbers should be left on answering machines and voicemail systems (or with the person that answers) if the person you are trying to reach is not available.

- If you use an answering machine, turn the volume down so that incoming messages cannot be overheard when left or played back.

- If use a voicemail system, protect your password and changed it periodically, just like your computer system password.

FAX MACHINE USE

Fax machines are still used for a broad range of sensitive information exchange, so security is critical:

- Whenever possible, fax users should rely on pre-programmed fax numbers set on the sending machine, to reduce dialing errors. *New fax numbers should be confirmed before first use.*

- Whenever possible, information should be sent only to fax machines at known locations, where the physical security of the receiving machine can be assured.

- All faxes containing sensitive information should include a confidentiality notice – requesting that faxes sent to an incorrect destination be destroyed, and requesting notification to the sender of such errors. *But do not rely on this alone to protect your fax!*

- Sensitive documents – inbound or outbound – should not be left sitting in or around the machine.

- Use conventional (postal service) mail when you can for communications with patients. Yes, it's slower, but it's generally more secure.

INFORMATION ON A COMPUTER

Information security requires protection of *every* computer. In a world where computers are networked together, a risk to one is a risk to all:

- Computers should be kept in physically secure, non-public locations whenever possible. Computers that must be in public areas should be positioned so they're safe from visitors.

- Be particularly careful that computer screens can't easily be seen by visitors.

- Keep backup copies of important information, but keep those backup copies safe. Storage media like floppies, CDs, flash memory cards and the like should be in secure locations too.

- When you're done with them, secure disposal of such storage media is *essential*. That includes the hard drive on the computer itself, when you decide to get rid of it.

- Basic security protections should be in place on every computer, like anti-virus and a firewall. At work you may not need to do this yourself, but you need to be sure it's been done by someone.

- If you're responsible for your own computer's security, see the "Protecting Your Computer" for the details of what you need to do.

COMPUTER ACCESS

- Most of computer systems rely on user-ids and passwords for security, so password discipline is one of the most critical rules:

  - Pick passwords that are hard to guess. And change them regularly.
  - *Don't* use the same password for every computer system you use.
  - If you write passwords down in order to remember them, keep that in a safe place! (And try not to write them down in the first place.)
  - If you think your password has been compromised, change it and *report the incident to the security department too!*
  - For more tips, see the "Picking and Protecting Passwords" course.

- If computer access tokens are used (such as USB keys), they should be kept with you, or in a safe place otherwise. *Report a lost or stolen access token immediately!*

- Log on to computer systems or terminals only with your own user-id, password or token. These should be "shared" only in true emergencies.

- Log off or lock your computer whenever you leave it unattended, even if just for a short time. Some of our systems will "time out" after a period of inactivity, but don't rely on that.

PORTABLE COMPUTERS, PDA/S, ETC.

Portable devices are extremely convenient, but also present a tremendous security risk:

- Whenever possible, portable computing devices should be kept secure in the facility, where physical security protections are better. (Did we mention that computer theft is common?)

- Avoid keeping a lot of sensitive data on portables that must leave the office. Rely instead on security-enabled communication links to on-site databases. *Violate this rule at your peril!*

- Security features on the portable device should be used, especially if it contains any kind of sensitive information. Portable storage like flash memory cards also require security attention.

- If a portable device containing sensitive information is lost or stolen, *report it immediately!*

- Safe computing with portables also requires following all the rules for non-portable computers. See the "Protecting Your Portables" course for more details.

ELECTRONIC MAIL USE

If it isn't used properly, email can present big security risks. Not all email is alike. Some systems are very secure, other systems aren't secure at all.

- Be careful about including any information that might be considered confidential in an email. Although most email gets to its destination safely, you cannot really control where yours will go, where or how long it will be stored, or who will see it.

- Be especially careful about sending file attachments. *And remember that file attachments you receive are a potential source of viruses and other malicious software.*

- If the information is confidential, include an appropriate confidentiality notice at the end of the message (similar to those used for faxes). *But do not rely on this alone to protect your email!*

- Re-read the email before you send it. Make sure the content is appropriate for the intended recipients. Consider who else might see the message.

- Always double-check that you have the correct "to" addresses. Be especially careful when you "reply to all" or add "cc"/"bcc" addresses.

- Unless you have access to a secure email service, use conventional (postal service) mail when you can for communications with patients. It's slower, but it's generally much more secure.

- For more details, see the "Kinder, Gentler, Safer Emailing" course.

INSTANT MESSAGING (IM)

IM is not as common as email in the workplace, but its use in increasing. Because of security, you may be restricted to using workplace IM systems, rather than popular IM clients from AOL, MSN, Yahoo, etc.

- As with email, be careful about sending confidential information via instant messages, either in the message itself or in an attached file.
- If you must send confidential information in an IM (despite our advice), language about confidentiality may need to be included.
- Even though it's an informal medium, take the time to re-read messages before you send. Like email, workplace IM can be considered official correspondence, and is subject to inspection.
- For more, see the "Safer Instant Messaging" course.

WEB SURFING

Web surfing is even more popular than email. Like email, it presents risks if not used safely.

- Workplace surfing is usually should generally be limited to your organization's own web pages and "safe" external sites that have information necessary for your work duties.
- Web browers need to have appropriate security settings. (This is true of all software.)
- Remember that your workplace web surfing, like all other computer activities, may be monitored.

FILE SHARING AND GAME PLAYING

- At work, just say no. Shared files are a common way to get infected by malicious software. Workplace computers shouldn't be used for "play." Keep in mind that you may be monitored.

SOCIAL ENGINEERING

Technical vulnerabilities are one source of problems, but human vulnerabilities are just as critical. Don't get conned into making a security mistake.

- Remember that it's much harder to confirm someone's identity in virtual world, so extra caution is always required.
- Be cautious any time you are asked for sensitive information, whether by phone, fax, email or even in person. Be particularly cautious when you are asked for passwords, PINs, account numbers or other personal data that is critical to establishing identity.
- Until you're sure about the propriety of a communication, just say no.
- For more on social engineering, see the "Protecting Your Identity" course.

►Questions and comments about this document are welcome. Send email to ethics@miami.edu.