## Frequently Asked Questions about HIPAA Privacy

Please use this page as a quick reference for frequently asked questions about HIPAA privacy. We welcome the opportunity to enhance this page with reliable information.

**Q. Who may access confidential information?**
A. Only those people who need access for business reasons and who have been authorized to receive it.

**Q. What is meant by having access to the "minimum necessary" information to do our jobs?**
A. We have access to all information that we need to do our jobs, but we should not have access to unnecessary information.

**Q. Who is our privacy officer? Who is our information security officer?**
A. Privacy Officer: Lynn Hutt and Information Security Officer: Bob Hogle

**Q. Why do we need privacy and security officers?**
A. They are responsible for the overall protection of patient privacy and the security of all our information, whether on paper, in the computer, or in conversation.

**Q. Who is responsible for maintaining a secure environment and patient privacy?**
A. Each one of us.

**Q. Who is responsible if I "lend" my password to my co-worker and she uses it to look up information on a friend she's concerned about?**
A. Both of us have violated our organization's policy. I am ultimately responsible for having shared my password.

**Q. May I discuss patients with my spouse if he/she doesn't work here and promises to keep it secret?**
A. No.

**Q. Am I permitted to look up my sick father's medical record?**
A. You are not permitted to look at your father's record unless your father has informed the hospital that that is okay. While parents usually want family involvement in their treatment, it shouldn't be assumed. Sometimes an individual does not want family members to know the details.

**Q. We know that diagnoses and test results are confidential. What other information about a patient is confidential? What about billing records?**
A. Essentially any information that is patient-identifiable, even the patient's address, is confidential and must be protected. Only when the patient has agreed may it be used or disclosed for specific purposes.

Also, removal of the patient's name does not mean the patient's identity is protected; other information such as a medical record number, a zip code, or a date of birth could still be used for identification.

**Q. What patient information can we disclose to any caller or visitor who asks?**
A. Name, hospital location, and general condition may be available to the public when the patient has agreed. Patients who have agreed are listed on the Directory Report in STAR. Patients who are listed as "confidential" in STAR do not want their information given out, and we must be careful not to let that happen. Be sure you know how to tell which patients have agreed and which have not.

**Q. What could happen to me if I talked about patients even though I no longer worked here?**
A. We are all required to keep patient information confidential "forever". A privacy breach could result in legal penalties even if you no longer work here.

**Q. Why does everyone have his or her own unique user ID (i.e., log-on ID, etc.)?**
A. Each person must have his or her own user ID so that he or she can be held accountable for activity connected to that ID.

**Q. What are some important rules for making up "good" passwords? Ones that are hard for someone else to guess?**
A. They should be at least eight characters long; contain both numbers and letters; never be a real word or a significant number string; never be the name of a fictional character, a car model, or such.

**Q. Is it okay to hide your password under your mouse pad or keyboard tray?**
A. No. Passwords "hidden" this way can be easily found. This is not taking reasonable care to keep your password secret.

**Q. What should you do if a well-known staff physician says that he has lost his password but needs immediate access to his patient's lab results and asks you to look up that patient's records for him?**
A. But you should let the physician know you are not comfortable in doing this. And you should report the incident to the security officer. Thus the physician can get his password restored, and you are on record for noting that the patient look-up was done at the physician's request.

**Q. What should you do if your computer access doesn't let you see information you need? Is it all right to ask a co-worker to share her password when the need is legitimate?**
A. You should talk to your manager and arrange for the necessary access. It is never permissible to use someone else's password.

**Q. What could happen to me if I talked about patients even though I no longer worked here?**
A. We are all required to keep patient information confidential "forever". A privacy breach could result in legal penalties even if you no longer worked here.

**Q. We know that medical records, whether paper or electronic are confidential. What about handwritten notes and phone calls?**
A. All forms of information, written, spoken, or electronic are confidential and must be protected.

**Q. What should you do if another organization asks for access to patient information in your computer system?**
A. Forward the request to your privacy (Lynn Hutt) or information security officer (Bob Hogle). This access must be closely scrutinized first.

**Q. How do you know what material is confidential?**
A. Hospital guidelines describe what information is confidential, including anything that could be used to identify a patient. Computer user IDs and access codes, payroll information, confidential memos, and many other documents are also considered confidential information. Please refer to MCO's confidentiality policy

**Q. How should you dispose of confidential papers?**
A. Put them in the locked shredder bin in your area. Please refer to MCO's Disposal of Confidential Information policy.

**Q. Is it all right to bring in software from home? Why or why not?**
A. Unless it has been approved and virus-scanned, it may contain a virus or other malicious code that could infect your PC and others on the network. Loading of software on PCs can also create issues with software necessary to do business which could render the PC inoperable. It is not in the interest of MCO to utilize unlicensed software, this creates legal issues

**Q. Why is it important to log off when you leave your PC, even if no one else is around?**
A. Even at the end of the day, housecleaning crews and others may be in the area and use your access - for which you will be held responsible!

**Q. Can you identify two ways to protect the information on your computer screen?**
A. Turn the screen away from public view. Use a password-protected screen saver that pops up after a few minutes of idle time and hides the information. Log off when you leave the area.

**Q. Why is it important to read the message when you log on that tells you the last time you logged on?**
A. If it was at an hour or on a day when you know you couldn't have logged on, someone else may have used your user ID and password. You must report this at once and change your password.