

This brochure provides basic information about the HIPAA Security Rule and how it affects the way we do our jobs.

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a Federal law passed by Congress that protects the privacy of an individual's medical information and was implemented by the Federal Department of Health and Human Services.

What Does HIPAA Cover?

- ⑥ Health care transactions like eligibility, authorizations, claims, and payments
- ⑥ Confidentiality and privacy of health information
- ⑥ Security of electronic systems that receive, maintain, and transmit health information

Who is Protected by HIPAA?

- ⑥ Persons receiving health care services provided by Orange County employees
- ⑥ Persons receiving health care services paid for by Orange County

What Information is Confidential?

Any information about the health of an individual, which identifies or can be used to identify the individual, is confidential. HIPAA applies to information communicated orally and in writing. It applies to information stored in hard copy or any electronic device or database, or is transmitted through any electronic means.

What is the HIPAA Security Rule?

The HIPAA Security Rule is the logical extension of the Privacy Rule. The Privacy Rule focuses on how people handle protected health information (PHI) in any form, the Security Rule covers the technical Security for PHI in electronic form (ePHI).

What is the purpose of the Security Rule?

The Security Rule requires that the County ensure the confidentiality, availability and integrity of the ePHI that we create, receive, maintain, or transmit. The Security Rule also requires ePHI be accessible to those who appropriately need it, when they need it.

When is it considered ePHI?

Protected Health Information is considered electronic PHI when it is being stored or “at rest” on a computer, on a server, on a floppy disk or a CD. It is also considered ePHI when it is “in transmission,” such as when you send an email.

How is ePHI protected?

The Security Rule requires that the County put technical controls in place to ensure that ePHI is protected from unauthorized access. Our Information Technology staff does that in many ways, including assigning unique user IDs and passwords for network access, reviewing audit logs of who is accessing e-PHI, having virus protection in place, backing up ePHI each day, and checking those backups for integrity. These are some of the technical measures required by the HIPAA Security Rule.

What does this mean to me?

You are the most important link in the security of ePHI. Security is more than a product or a set of policies, and it requires the consistent effort of a well-informed and diligent workforce.

Can I send ePHI through email?

The Security Rule requires that we protect ePHI, and an email in transmission is not secure unless proper safeguards are applied. The email you send can be intercepted and read by an unauthorized individual at any point in transmission. Also, emails can be sent to the wrong person. Once you press the “send” button, it is out of your control. Before sending ePHI through email, first ask yourself if the PHI must be sent by email, or if another option is available. If email must be used, one option is to send the PHI in a password protected document, and send the password in a separate email. NEVER put PHI in the subject line of an email.

Why is my desktop PC an unsecured environment?

PHI stored on your hard drive is easily accessible to anyone using your PC. Storing ePHI on servers allows Information Technology staff to implement technical access controls, such as unique user IDs and tough passwords. If ePHI must be maintained on your desktop PC or a laptop

computer, it is essential that you work with Information Technology staff to develop specific protocols to secure the ePHI stored on that equipment.

Why do I have to use such a complicated password?

There are people who spend time trying to “crack” passwords and gain unauthorized access to information that you have. A simple four to six letter lower case password can be “cracked” in only a few minutes. A password with eight or more upper and lower case letters and numbers with a special character is significantly more difficult to “crack.” NEVER share your password, not even with your supervisor. If others know your password, change it immediately.

What else can I do to protect ePHI?

Be aware of the ePHI in your care, and follow the Security policies and procedures to protect and secure that ePHI. Do not remove ePHI to an unsecured environment, such as your desktop PC, a laptop computer, or your home PC.

- ⑥ If you work with confidential information on your computer, make sure you log off before leaving it unattended. All computers should be locked when not in use. Never share your computer password and don't leave it lying around.
- ⑥ Make sure your computer screen is not easily viewed by the public or other employees.
- ⑥ Don't transmit confidential information by email unless it is absolutely necessary and then only if zipped and password-protected. If your computer has encryption capability, all confidential email should be encrypted.
- ⑥ Avoid downloading software from the Internet.
- ⑥ If you share a computer, always log off before someone else logs on.
- ⑥ If you must write down your password, store it in a safe place. Do not post it on your monitor, place it under your keyboard, or put it in an easily accessible location.

If you have questions or would like a copy of the Rule, please visit the County of Orange website at: www.ocgov.com/hipaa. You may contact the HCA HIPAA Coordinator by phone at (714) 834-4082 or by email at hipaa@ochca.com. You may contact the County HIPAA Security Officer by phone at (714) 834-2040 or by email at securityofficer@ocgov.com. You may contact the County HIPAA Privacy Officer by phone at (714) 834-5172 or by email at privacyofficer@ocgov.com.



HIPAA Security Primer

