OFFICE FOR CIVIL RIGHTS

PRIVACY, SECURITY, AND ELECTRONIC HEALTH RECORDS

Your health care provider may be moving from paper records to electronic health records (EHRs) or may be using EHRs already. EHRs allow providers to use information more effectively to improve the quality and efficiency of your care, but EHRs will not change the privacy protections or security safeguards that apply to your health information.

EHRs and Your Health Information

EHRs are electronic versions of the paper charts in your doctor's or other health care provider's office. An EHR may include your medical history, notes, and other information about your health including your symptoms, diagnoses, medications, lab results, vital signs, immunizations, and reports from diagnostic tests such as x-rays.

Providers are working with other doctors, hospitals, and health plans to find ways to share that information. The information in EHRs can be shared with other organizations involved in your care if the computer systems are set up to talk to each other. Information in these records should only be shared for purposes authorized by law or by you.

You have privacy rights whether your information is stored as a paper record or stored in an electronic form. The same federal laws that already protect your health information also apply to information in EHRs.

Benefits of Having EHRs

Whether your health care provider is just beginning to switch from paper records to EHRs or is already using EHRs within the office, you will likely experience one or more of the following benefits:

- **Improved Quality of Care.** As your doctors begin to use EHRs and set up ways to securely share your health information with other providers, it will make it easier for everyone to work together to make sure you are getting the care you need. For example:
  - Information about your medications will be available in EHRs so that health care providers don't give you another medicine that might be harmful to you.
  - EHR systems are backed up like most computer systems, so if you are in an area affected by a disaster, like a hurricane, your health information can be retrieved.
  - EHRs can be available in an emergency. If you are in an accident and are unable to explain your health history, a hospital that has a system may be able to talk to your doctor's system. The hospital will get information about your medications, health issues, and tests, so decisions about your emergency care are faster and more informed.

- **More Efficient Care.** Doctors using EHRs may find it easier or faster to track your lab results and share progress with you. If your doctors' systems can share information, one doctor can see test results from another doctor, so the test doesn't always have to be repeated. Especially with x-rays and certain lab tests, this means you are at less risk from radiation and other side effects. When tests are not repeated unnecessarily, it also means you pay less for your health care in copayments and deductibles.
- **More Convenient Care.** EHRs can alert providers to contact you when it is time for certain screening tests. When doctors, pharmacies, labs, and other members of your health care team are able to share information, you may no longer have to fill out all the same forms over and over again, wait for paper records to be passed from one doctor to the other, or carry those records yourself.

Keeping Your Electronic Health Information Secure

Most of us feel that our health information is private and should be protected. The federal government put in place the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to ensure you have rights over your own health information, no matter what form it is in. The government also created the HIPAA Security Rule to require specific protections to safeguard your electronic health information. A few possible measures that can be built in to EHR systems may include:

- "Access control" tools like passwords and PIN numbers, to help limit access to your information to authorized individuals.
- "Encrypting" your stored information. That means your health information cannot be read or understood except by those using a system that can "decrypt" it with a "key."
- An "audit trail" feature, which records who accessed your information, what changes were made and when.

Finally, federal law requires doctors, hospitals, and other health care providers to notify you of a "breach." The law also requires the health care provider to notify the Secretary of Health and Human Services. If a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction. This requirement helps patients know if something has gone wrong with the protection of their information and helps keep providers accountable for EHR protection.

To learn more, visit **www.hhs.gov/ocr/privacy/**.

For more information, visit **www.hhs.gov/ocr**.

U.S. Department of Health & Human Services
Office for Civil Rights