Health Information Technology: **Privacy** and **Security**

This publication is made possible through the Health Information Security and Privacy Collaboration.

www.eHealthWV.org

e-HealthWV
Your care. Your future. Learn more.

Electronic Health Records and Security

As we enter the digital age, physicians and other medical providers are moving from paper health records to electronic health records. Other industries, such as banking, have already made the switch to electronic record systems.

Providers with electronic health records can join networks for health information exchange (HIE). This could mean that your cardiologist could get your health records from your primary care physician electronically. In the future, if you have a medical emergency while traveling, the treating physician might be able to access your records via computer. That would help ensure proper medical care.

These new advancements in health record technology raise questions about security and privacy. Consumers may be concerned that someone may be able to hack into health systems to gain access to private health information.

Federal and state privacy laws, such as HIPAA, are designed to protect both paper and electronic health records. Systems must be designed to meet these stringent requirements. Any certified electronic system must be password protected and able to be encoded so that only authorized individuals can read the health records.

Unlike with paper health records, a log is created every time someone views a health record electronically. In addition, access to certain parts of health records can be regulated by password and system design.

The following privacy and security principles should be part of any electronic health record system:

- Individuals should know how their personally identifiable health information may be used and who has access to it.
- Individuals should have control over whether and how their personally identifiable health information is shared.
- Systems must protect the integrity, privacy, security and confidentiality of an individual's information.
- The governance and administration of electronic health information exchanges and networks should be transparent and publicly accountable.

For more information on privacy, visit our Web site: www.eHealthWV.org.

Electronic health records offer a safety feature that is not available with paper records. Electronic copies known as backups can be easily made and stored off site. In the case of flood, fire or other natural disasters, a physician's office can be destroyed. If a disaster hits, a medical practice with electronic health records can be re-established quickly.

A physician who has an electronic system with regular backups will be able to re-establish the office with all patient and financial records intact. This is good for patient care and the financial well-being of the medical practice.