Your Health Information Privacy and Security

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules establish Federal requirements for keeping your health information secure. The HIPAA Privacy Rule generally requires health care providers and health plans to safeguard your health information. This requirement applies to both paper and electronic records. The HIPAA Security Rule more specifically details the steps your health care providers and others must take to keep your electronic protected health information secure.

Is all of my health information protected by HIPAA?

Privacy protections apply to your "individually identifiable health information," which means:

- Information that relates to your past, present, or future physical or mental health or condition; to the provision of health care to you; or to past, present, or future payment for the provision of health care to you

- Information that identifies you or for which there is a reasonable basis to believe it can be used to identify you

This information can include:

- Information your doctors, nurses, and other health care providers put in your medical record

- Conversations your doctor has about your care or treatment with nurses and others

- Billing information about you

- Information used by companies or individuals that provide data, billing, or other services to doctors, hospitals, health insurers, and other health care organizations

When this information is held by an individual or organization that must follow HIPAA, it is called "protected health information."

What are some of the safeguards Baptist Health uses to protect my health information when it is stored in an electronic health record?

In keeping with the HIPAA Privacy and Security Rule, some of the safeguards Baptist Health has taken to protect patients' protected health information include:

- A risk management program to assess security risks and if necessary, to develop and execute action plans to mitigate those risks

- Established policies and procedures to prevent, detect, contain, and correct security and privacy violations
- Implemented security measures to reduce risks and vulnerabilities such as firewalls, intrusion prevention system, disk encryption, anti-virus/anti-malware protection on servers and workstations, two-factor authentication for remote access to information systems, and regular system patches and upgrades
- Agreements with service providers and business associates to ensure that they only use and share your health information according to the law
- Established policies and procedures to limit who can access your health information as well as training programs for employees about how to protect your health information
- Audit trails that record who accessed your information, what changes were made, and when they were made

What happens if there is a breach of my health information?

Baptist Health strictly adheres to the HIPAA Breach Notification Rule which requires doctors, hospitals, other health care providers, and health insurance companies to notify you of a "breach" if unsecured information about you is seen by someone who is not supposed to see it. This Federal law also requires health care providers and insurance companies to promptly notify the Secretary of the U.S. Department of Health and Human Services if there is any breach of unsecured protected health information and notify the media and public if the breach affects more than 500 people.

This requirement helps patients know if unsecured protected health information has been breached and helps keep providers accountable for the protection of your health information.

How can I learn more about how Baptist Health uses and discloses my protected health information?

The Baptist Health Notice of Privacy Practices includes important information that describes how medical information about your may be used and disclosed and how you can get access to this information. A hard copy of the Notice of Privacy Practices can be obtained by calling the Baptist Health Privacy Office at 786-596-8850. An electronic copy of the Notice of Privacy Practices is available at: www.baptisthealth.net/en/privacy-information/pages/default.aspx

If you have any questions about the security, use, disclosure or access to your protected health information at Baptist Health, you may contact the Baptist Health Chief Privacy Officer at 786-596-8850 or toll-free at 1-866-33-HIPAA (44722).