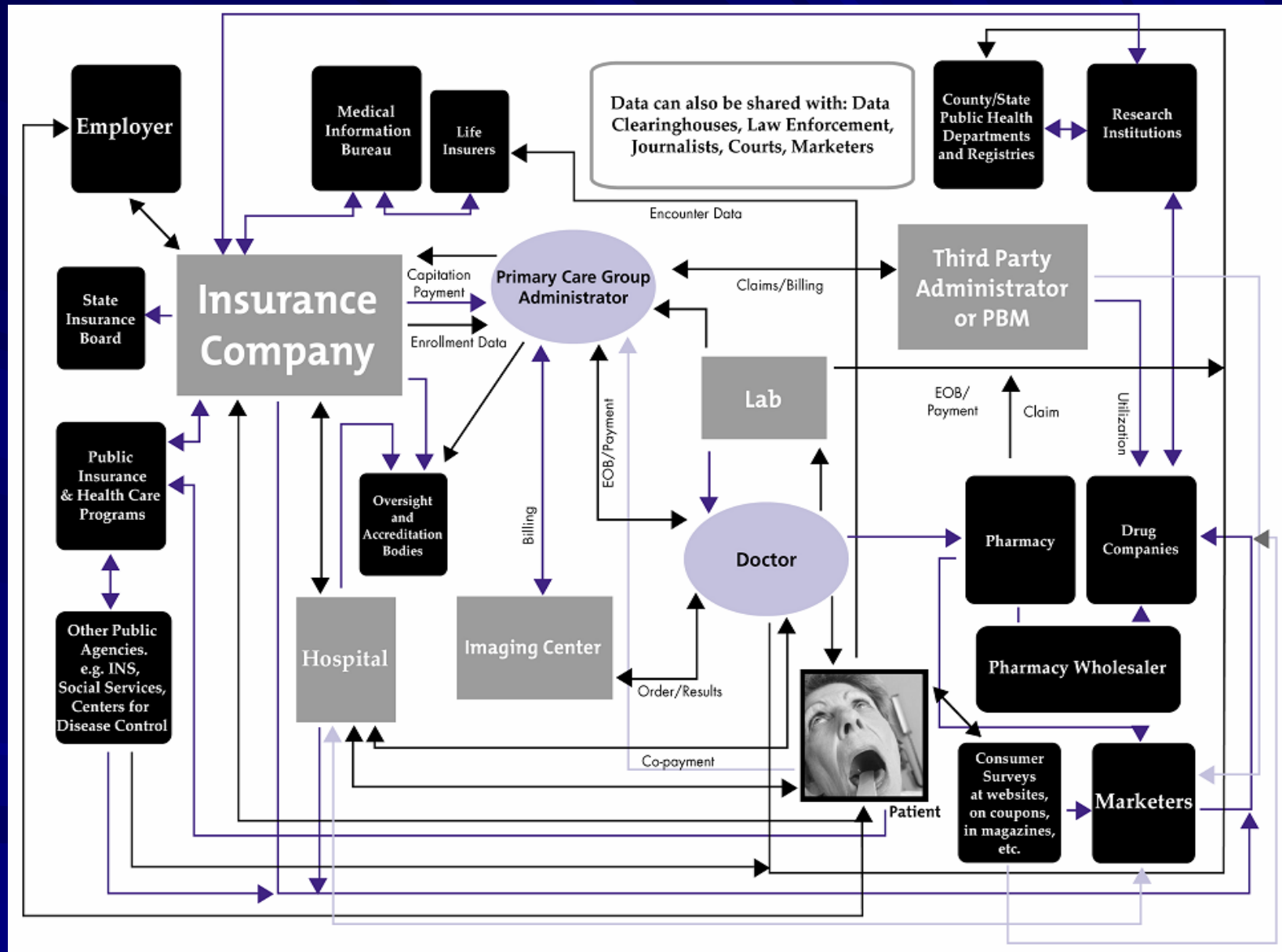


**HIPAA:  
Federal Regulations  
Governing Patient  
Privacy**

# Why are privacy protections needed?

- Increasing public concern about loss of privacy
- Broad availability of information stored and exchanged in electronic format
- Concerns about genetic information
- A conflicting patchwork of state laws

# Exchanging Health Information in the 21<sup>st</sup> Century



# HIPAA

The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes comprehensive protections for medical privacy.

The **Privacy Rule** governs a provider's use and disclosure of health information and grants individuals new rights of access and control. The regulation also establishes **civil and criminal penalties** for violations of patient privacy.



# The Privacy Rule is Founded on Two Very Basic Principles:

- Health information belongs to the patient.
- Patients have a right to know how their information is being used.

## **Under the Privacy Rule, patients have the following new rights:**

- Receive a Notice of Privacy Practices from their provider
- Access, inspect and copy their medical records
- Request corrections to their medical record
- Request special accommodations on how their health information is communicated (such as alternate addresses and phones)
- Request restrictions on how their information is used
- Receive an accounting of non-routine disclosures
- “Opt-out” of inclusion in facility directories and fundraising efforts
- File a complaint to the institution and to the federal Department of Health and Human Services

# HIPAA: The Terminology

- Covered entity
- Protected Health Information (PHI)
- Use and disclosure
- Role-based access
- Minimum necessary

**“Covered Entities”** are the groups or individuals **who** have to comply with the law\*

- Health plans
- Health care clearinghouses
- Health care providers who conduct electronic transactions related to third-party billing

\*Regulations also apply to vendors who perform a business function using the covered entity's patient information.

# The Privacy Rule Governs Protected Health Information (PHI)

PHI is any information that is:

- Created or received by a covered entity; and
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual and which:
  - identifies the individual; or
  - offers a reasonable basis for identification of the individual

# The law establishes rules about the use and disclosure of PHI

- **“Uses”** take place within the organization holding the medical information.
- **“Disclosures”** are releases to parties external to the organization.

# Health Care Providers are required to ensure “Role-based Access”

- Covered entities must identify which persons in the organization need access to PHI in order to fulfill their duties.
- Covered entities must limit the PHI used or disclosed to the **minimum necessary** to achieve the purpose of the use or disclosure.
  - **Note:** The minimum necessary standard does not apply to disclosures made for treatment purposes or disclosures to the individual patient.

# **KU Medical Center must meet HIPAA requirements in four major areas:**

- Clinical requirements
- Research requirements
- Computer security
- Institutional requirements

# **Basic Requirements:**

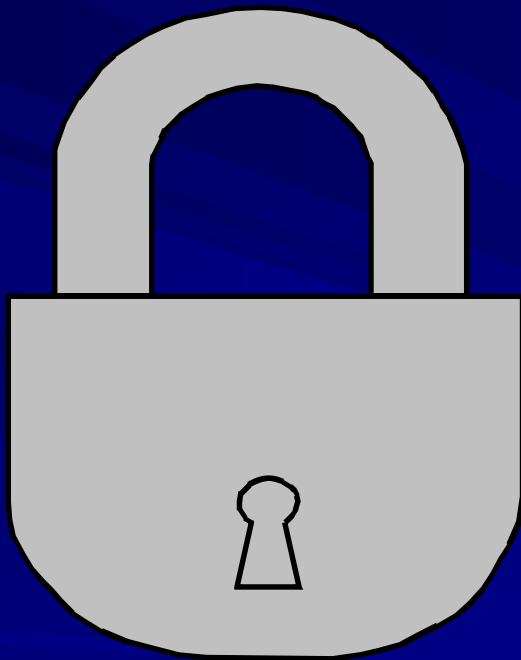
## **Clinical Issues**

- **Deliver the KUMC Notice of Privacy Practices** to our patients.
- Limit uses and disclosures in accordance with legal requirements
- Accommodate privacy requests from patients
- Maintain an accounting system to track non-routine disclosures

# Basic Requirements: Research Issues

- The KUMC Human Subjects Committee must make a privacy determination when conducting the ethical review of each study.
- HSC approval will include HIPAA approval.
- The informed consent form must include required statements about privacy protections.
- HIPAA requires new approval criteria for database studies and retrospective chart reviews.

# Basic Requirements: Computer Security



- Locate computer systems containing PHI
- Install firewalls for data integrity
- Encrypt internet transmissions of PHI
- Maintain password protections on files containing PHI
- Limit access to patient files, based upon job duties

# Basic Requirements: Institutional Issues

- Designate a Privacy Official
- Develop policies and procedures
- Train all workforce members
- Establish a complaint mechanism
- Enforce sanctions (civil and criminal penalties)

# The “Take-Home” Message

- Remember that patient information ultimately belongs to the patient, not the provider.
- Our commitment to patient care includes a commitment to respecting patients’ rights of privacy.
- All KUMC employees and trainees must follow the institution’s policies for handling and releasing patient information.

# Proposed Benefits of the Privacy Rule

- The Privacy Rule establishes the first comprehensive federal protections for health information.
- Patients will have increased access and control over their records.
- The Privacy Rule supports the creation of new electronic standards that will make health care billing more efficient.
- The Privacy Rule strikes a balance between individual rights and the need for information in public health and research.

# New privacy rights for patients go into effect on April 14, 2003

For questions, contact:

Karen Blackwell, MS

[kblackwe@kumc.edu](mailto:kblackwe@kumc.edu)

913.588.0940

Tom Field, MEd

[tfield@kumc.edu](mailto:tfield@kumc.edu)

913.588.0942

