

A photograph of the North Kansas City Hospital building at dusk. The building is a multi-story structure with a brick facade on the left and a modern glass and metal facade on the right. The sky is a deep blue. A large illuminated sign on the brick part of the building reads "North Kansas City Hospital".

North  
Kansas City  
Hospital

# HIPAA for the General Workforce

What You Need to Know



*Where your care  
is personal.*

# Education Objectives

- Understand the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations
- Understand the penalties for non-compliance
- Understand patients' rights and healthcare workers' roles in protecting them
- Understand your responsibilities under HIPAA-related policies and procedures

# The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- HIPAA is a federal law imposed on all healthcare organizations, including:
  - Hospitals, physician offices, home health agencies, nursing homes and other healthcare providers
  - Clearinghouses
  - HMOs, private health plans and public payers such as Medicare and Medicaid
- The above organizations are considered “Covered Entities” under HIPAA

# Individual Rights

- Patients have the following rights under HIPAA:
  - **Notice of Privacy of Practices**
    - To know who has access to their health information and how it is used
  - **Access and Amendment**
    - To access and request an amendment to their health records in the designated record set

# Individual Rights

## – Accounting of Disclosures

- To request a list of people and organizations who have received his/her health information

## – Confidential Communications

- To request we communicate with them by alternative means

## – Request Restrictions

- To request restrictions for the use and disclosure of their health information



# Individual Rights

## – Complaints

- To complain to a covered entity, the Secretary of HHS or the Office for Civil Rights (OCR)

# What is Confidential?

- Protected Health Information (PHI) is any information about a patient
  - Written/printed on paper, saved electronically or spoken
- Name
- Address
- Age
- Social Security number
- Phone number
- E-mail address
- Diagnosis
- Medical history
- Medications
- Observations of health
- Medical record number
- And more...

# Protect Patient Privacy “Do’s”

- Lock your computer when you walk away, or log off the computer when you’re finished.
- Dispose of health information only by shredding or storing in locked containers for destruction.
- Notify Security if you see an unescorted visitor in a private area.



# Protect Patient Privacy “Don’ts”

- Don’t leave patient records lying around.
- Don’t discuss a patient in public areas such as elevators, hallways and cafeterias.
- Don’t look at information about a patient unless you need it to do your job.

# Do You Need to Know? The Minimum Necessary Standard



*Where your care  
is personal.*



# Do You Need to Know?

HIPAA requires healthcare workers to use the minimum amount of health information they need to do their jobs efficiently and effectively

- **Ask yourself:**

- Do I need this information to do my job and provide good service?
- What is the least amount of information I need to do my job?

# Do You Need to Know?

- Coders and billers
  - Need to look at certain portions of records to code and bill correctly
- Professional healthcare workforce members such as doctors, nurses and therapists
  - Need to look at their patients' records to care for them

# Do You Need to Know?

- Housekeeping staff
  - Do not need to look at patient records to perform their job
- Caregivers
  - If no longer caring for a patient, they do not need to look at that patient's information to perform their job
  - Do not need to look at patient lists for areas in the hospital in which they are not working

# Do You Need to Know?

- Employees
  - Do not need to look at their own records

# Access and Disclosure



*Where your care  
is personal.*



# Use of PHI

- Patient information may be used for treatment, payment or healthcare operations without an authorization.
- For other uses, we must obtain an authorization.
  - Examples of other uses include marketing, fundraising, research, employment determinations and patient-directed disclosures.



# Use of PHI

- A patient may revoke an authorization at any time by making a written request.

# Examples of Treatment, Payment and Healthcare Operations

- **Treatment**
  - Doctors and nurses caring for patients; technicians performing tests
- **Payment**
  - Billers sending out claims; coders applying codes to procedures
- **Healthcare operations**
  - Quality assurance staff performing reviews; transcriptionists typing reports



# Authorization Exceptions

- An authorization is not necessary for uses or disclosures mandated by law such as:
  - Reporting births, deaths and communicable diseases to state agencies
  - Giving certain information to the police for investigations and searches for missing people

# Authorization Exceptions

- Responding to a court order, subpoena or other lawful process
- External health oversight agencies
- Public health activities
- Abuse/neglect reporting
- Organ donation

# The Facility Directory

- Unless a patient has asked to be excluded from the directory, you may disclose the following information to visitors and callers who ask for a patient listed in the directory by name:
  - Location (room number)
  - General condition (e.g. stable, critical)

# The Facility Directory

- A patient may opt out of the directory and become a “no information” patient.
- For celebrity patients or other media inquiries, refer callers to the Marketing Department or Director of Clinical Operations



# Patient Spokesperson

- Patient information should be shared only with the patient and the two designated spokespersons.
- Nurse performing the admission assessment will ask the patient to identify two spokespersons
- “Spokesperson” is not a legal designation (such as a DPOA or guardian).

# Patient Spokesperson

- Share the minimum information requested by the spokesperson.
- Other callers may be directed to talk with the patient or the spokesperson(s).



# Social Media

- Avoid “friending” patients and/or their family.
- Do not post any reference to any patient on any social site.
  - Leaving off the name of the patient does not make it OK.
- Do not post any photos online that include patients or patient information.

# Protecting ePHI



*Where your care  
is personal.*



# HIPAA Security Rule and ePHI

- Applies to protected health information that is electronically (ePHI) sent from one location to another or stored by the facility
- Identifies steps to take to secure electronic PHI

# Information Security

- The security rule has three key areas that work together to protect PHI, which include:
  - Physical safeguards
  - Technical safeguards
  - Administrative safeguards

# Physical Safeguards

- Help protect the physical computer systems and related buildings and equipment from unauthorized access, fire and other natural and environmental hazards
- Some physical safeguards were discussed in the privacy section of this course and included access to computer systems and workstations.

# Technical Safeguards

- Steps and procedures that must be in place to:
  - Protect the integrity of electronic PHI
  - Control access
  - Audit for inappropriate access or use of records
  - Validate the identity and authorization of users
  - Protect electronic PHI transmitted over a communications network

# Technical Safeguards Examples

- Unique user IDs
- Reliable user authentication – typically passwords
- Encrypt emails containing PHI
- Authorization to access information
- Automatic computer logoff (inactivity timeout)
- Firewalls
- Log capture and monitoring

# Passwords

## The First Layer of Protection

- Password Selection Best Practices

- Follow Password Guidelines in orientation packet. (Password Management Policy is on the Intranet.)
- Choose passwords that are difficult to guess.
- Don't use names of family members or pets.
- Don't use personal information (date of birth, license plate number, telephone number, Social Security number, make of automobile or home address).



# Passwords

## The First Layer of Protection

- Password Selection Best Practices
  - Don't use your first, middle or last name.
  - Don't use your User ID.

# Administrative Safeguards

- Under the security rule, policies and procedures must be in place that define the steps to address:
  - Adding, changing or deleting user access based on job responsibilities or if user terminates employment
  - Use and assignment of individual user IDs and passwords
  - How to access the computer system and/or electronic PHI in the event of an emergency

# Tips for Electronic Security

- Never share your password.
- Turn computer screens away from public view.
- Change your password every 180 days or as required by internal policy.
- Do not log into the system using someone else's password.
- Do not remove equipment or media containing ePHI from hospital property.

# Complaints and Privacy Incidents



*Where your care  
is personal.*



# Complaints and Grievances

- If a patient or family member complains his/her privacy has been “violated,” **IT IS YOUR RESPONSIBILITY** to make sure the concern is appropriately reported.
- If you receive a complaint, please notify your supervisor and complete the “Breach Report” under Online Forms/Service Forms on the Intranet.

# Complaints and Grievances

- Report ALL privacy complaints, not just those that you think are “serious” or “legitimate.”

# Privacy Incidents

- If you know an inappropriate disclosure occurred, follow these steps:
  - Mitigate disclosure - contact recipient to confirm destruction of the document(s) or return of document to NKCH
  - Notify Supervisor and/or Director
  - Complete the Breach Report under Online Forms/Service Forms on the Intranet
  - Report events promptly - every reported breach must be investigated within 60 days

# Privacy Incidents

- Every breach report is reviewed by the Privacy Officer to determine appropriate follow up.
- Report ALL privacy complaints, not just those that you think are “serious” or “legitimate.”



# Penalties



*Where your care  
is personal.*



# Penalties for Breaking the Privacy Rules

- **Criminal penalties under HIPAA**
  - Maximum of 10 years in jail
  - Criminal penalties can be assessed by the federal courts for simply “snooping.”
- **Civil penalties under HIPAA**
  - Maximum fine of \$50,000 per violation, up to a maximum of \$1.5 million for identical Provisions during a calendar year

# Penalties for Breaking the Privacy Rules

- Organization actions
  - Employee disciplinary actions include suspension and/or termination for serious violations of the organization's policies and procedures.

# Confidentiality Agreement

- By signing the Employee Handbook acknowledgment you agree to:
  - Dispose of health information properly.
  - Follow the organization's policies and procedures.
  - Access protected health information only when necessary to perform your job duties.
  - Share confidential information only with those who need the information to do their jobs.
  - Handle health records carefully to preserve individual privacy.

# Expert Resources at NKCH

Your Director

Privacy Officer

Karen Reynolds, ext. 1590

[Karen.Reynolds@nckh.org](mailto:Karen.Reynolds@nckh.org)

Compliance Director

Lisa Larson-Bunnell, ext. 5490

[Lisa.Larson-Bunnell@nkch.org](mailto:Lisa.Larson-Bunnell@nkch.org)

Compliance Officer

Jennifer Kozinn, ext. 2038

[Jennifer.Kozinn@nkch.org](mailto:Jennifer.Kozinn@nkch.org)

Security Officer and Chief Information Officer

Kristen Guilluame, ext.2082

[Kristen.Guilluame@nkch.org](mailto:Kristen.Guilluame@nkch.org)

Security Coordinator

Eric Behrens, ext. 2580

[Eric.Behrens@nkch.org](mailto:Eric.Behrens@nkch.org)



*Where your care  
is personal.*

# Questions



*Where your care  
is personal.*

