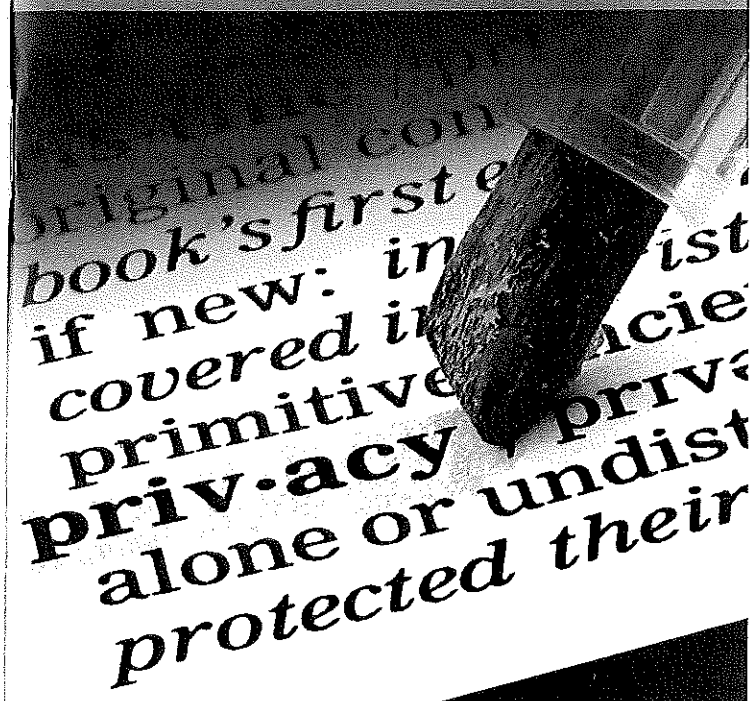
CROZER-KEYSTONE
HEALTH SYSTEM



Guidelines

for Protecting Patient Privacy and Information Security

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

Introduction

In the course of providing patient care, Crozer-Keystone Health System(CKHS) employees and medical staff use and share important and confidential information on a daily basis. CKHS is committed to ensuring the security of this information as well as maintaining patient privacy in accordance with state and federal laws and effective patient care. Everyone associated with CKHS plays a role in achieving these goals.

This guide provides an overview of the rules that CKHS staff must follow to protect patient information. It also describes steps to make sure that information remains secure and it explains how to report a breach in patient privacy or information security.

Staff are encouraged to carefully read this guide. Questions about the guide can be directed to the Corporate Compliance helpline at 1-800-387-7921.

Introduction to HIPAA

What is the Health Insurance Portability and Accountability Act ("HIPAA")?

HIPAA is a Federal law enacted to:

- Protect the privacy of patients' personal and health information
- Provide for the physical and electronic security of health information
- Simplify billing and other transactions related to health services
- Spell out the rights of patients regarding the use of their health information

What are the basic HIPAA requirements for CKHS staff?

Take reasonable measures to protect the privacy and security of our patient's Protected Health Information ("PHI")

Use only the amount of PHI that is "minimally necessary"

Respect rights of patients related to the use of their PHI

What Patient Information Must We Protect?

We must protect all information (written, spoken and electronic) that identifies the patient and relates to:

- the patient's physical or mental health or condition
- the provision of health care to the patient
- payment for the provision of health care to the patient
- and that includes one or more of 18 personal identifiers.

Protected Health Information ("PHI") Identifiers

- Names
- Postal Address
- All elements of dates (except year)
- Telephone numbers
- Fax numbers;
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code,.

When may we use and disclose PHI?

Generally, we must obtain the patient's written authorization to use and disclose PHI. However, we may use and disclose PHI without the patient's written authorization for the following purposes or situations.

Treatment, Payment, Health Care Operations. CKHS may use and disclose PHI in the following activities:

- **Treatment** is the provision, coordination, or management of health care and related services for a patient.
- **Payment** means our efforts to obtain payment for the provision of health care services to a patient.
- Health Care **Operations** are any of the following activities:
- quality assessment and improvement activities, including case management and care coordination
- competency assurance activities, including evaluation, credentialing, and accreditation
- conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs
- specified insurance functions, such as underwriting, risk rating, and reinsuring risk
- business planning, development, management, and administration
- business management and general administrative activities and certain fundraising for the benefit of CKHS.

Informal Permission. Where the patient is able to give informal permission or when it is clear from the circumstances that an incapacitated patient would likely provide permission if he/she were able to do so, we may use and disclose PHI when that is in the best interests of the patient.

Facility Directories. The Facility Directory is the list of hospital inpatients that is used by front desk staff and telephone operators to answer questions from people who want to visit or call patients. CKHS may rely on a patient's informal permission to list in its Facility Directory the patient's name, general condition, religious affiliation, and location in the hospital.

For Notification and Other Purposes. CKHS may disclose PHI to the patient's family, relatives, or friends, or to other persons whom the patient identifies.

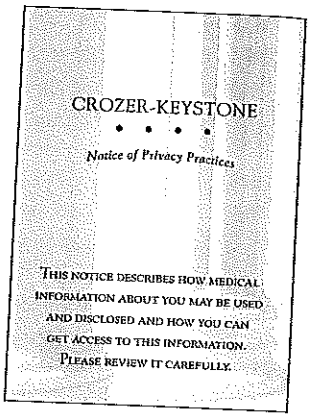
Incidental Use and Disclosure. A use or disclosure of PHI that occurs as a result of an otherwise permitted use or disclosure is permitted as long as we have taken reasonable safeguards.

Public Interest and Benefit Activities. We may use and disclose PHI in the following circumstances:

- When Required by Law.
- In Connection with Public Health Activities.
- To Report Abuse, Neglect or Domestic Violence.
- As Part of Health Oversight Activities.
- In Judicial and Administrative Proceedings.
- For Law Enforcement Purposes.
- To Provide Information about Deceased Patients to Coroners, Medical Examiners and Funeral Directors
- To Facilitate Donation of Cadaveric Organ, Eye, or Tissue
- Some Types of Research
- To Prevent or Lessen Serious Threat to Health or Safety.
- For Certain Essential Government Functions
- To Comply with Workers' Compensation

What does "Minimum Necessary" mean?

CKHS must make reasonable efforts to use and disclose the minimum amount of PHI needed to accomplish the intended purpose of the use or disclosure.



CKHS has policies and procedures to reasonably limit uses and disclosures to the minimum necessary.

Limited Access to PHI

CKHS restricts access to PHI to those people who need access to carry out their duties in taking care of patients.

Notice of Privacy Practices and Patients' Rights

CKHS provides information to its patients that describes the ways in which CKHS may use and disclose PHI. This Notice of Privacy Practices also describes patient rights related to PHI including the right to complain to HHS and to CKHS if they believe their privacy rights have been violated.

What patient rights does the Notice of Privacy Practices specify?

Access. Except in certain circumstances, patients have the right to review and obtain a copy of their PHI.

Amendment. HIPAA gives patients the right to ask CKHS to amend their PHI when that information is inaccurate or incomplete.

Disclosure Accounting. Patients have a right to obtain a list of the people to whom CKHS disclosed their PHI.

Restriction Request. Patients have the right to request that CKHS restrict use or disclosure of PHI. If we agree to the requested restriction, CKHS must comply with the agreed restrictions, except for purposes of treating the patient in a medical emergency.

Confidential Communications Requirements. CKHS permits patients to request an alternative means or location for receiving communications of PHI by means other than those that CKHS typically employs. For example, a patient may request that CKHS communicate with the patient through a designated address or phone number. Similarly, a patient may request that CKHS send communications in a closed envelope rather than a post card.

Behavioral Health Patients

Additional State and Federal regulations that are more restrictive than HIPAA apply to PHI related to behavioral health services and drug and alcohol treatment facilities. These laws require providers to obtain special written authorization by the patient before PHI may be used or disclosed. Employees who work in CKHS behavioral health services receive additional training on these regulations.

HIPAA Security Requirements

Introduction

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

A major goal of the HIPAA Security Rule is to protect the privacy of individuals' electronic health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.

General Security Rules

HIPAA requires CKHS to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI stored electronically ("e-PHI").

Specifically, CKHS must:

- Ensure the confidentiality, integrity, and availability of all e-PHI we create, receive, maintain or transmit;
- Identify and protect against threats to the security or integrity of the information;
- Protect against impermissible uses or disclosures; and
- Ensure compliance by CKHS staff

HIPAA also promotes the goals of maintaining the integrity and availability of e-PHI. "Integrity" means that e-PHI is not altered or destroyed in an unauthorized manner. "Availability" means that e-PHI is accessible and usable on demand by an authorized person.

Complying with the HIPAA Security Requirements

What Steps Must CKHS Staff Take to Safeguard Computer Resources and PHI?

There are several steps that staff must take to help protect the privacy and electronic security of PHI, several of which are listed below:

Password Security

- Protect your user ID and password. Do not share or post passwords under any circumstances!
- Commit your password to memory.
- When choosing passwords, at a minimum, incorporate a combination of letters and numbers into the password.
- Immediately change your password if it is accidentally exposed or compromised.
- Report all password exposures to your department supervisor or manager, or the CKHS Information Services (IS) Customer Support Line at 610-447-2610.
- Adhere to established password management guidelines by changing your password periodically and by following instructions when you think your password has been compromised.
- Always keep computers password-protected and under lock and key when not in use.

Workstation Security

- Log-off or lock access to computers when you leave.
- Keep confidential or sensitive information locked away when not in use. File documents in locked cabinets or drawers when you have finished with them.

- Ensure that displays of computer stations with access to e-PHI are not visible to unauthorized individuals.

- Be alert to recognize and report all privacy and security incidents to your department supervisor or manager, the CKHS compliance helpline and for information security issues call the IS Customer Support Line.

Disposal/destruction methods

- Never leave sensitive or confidential information in a trash bin. Securely dispose of all papers that contain PHI. ALWAYS follow the proper paper disposal procedure (e.g., use secure bags, shredders, locked 'shred-it' bins, etc.). Locked, shredder disposal bins are located throughout CKHS.

- Back up data files and securely store backup media; and follow approved CKHS media destruction before permitting devices and media to be transferred, sold or donated. Maintain records to track the movement (transfer or relocation) of devices and media.

Facility/Physical Access and Identification

- Always follow established visitor security procedures.

- Always wear your security badge/identity badge when at work.

PHI and E-mail, Telephones and Other Technologies

E-mail

Avoid using e-mail to send, receive or store confidential information.

- DO NOT send e-mail messages with patient information to users who do not have a "crozer.org" e-mail address unless such messages are encrypted and secure. Be aware that using a password is NOT data encryption.

- E-mail with patient information sent outside the "crozer.org" system must be protected with an approved CKHS e-mail data encryption solution. If you are not familiar with what method to use, contact IS.

- Use the same care in sending e-mails that you would with a letter. Do not write anything in an e-mail that you might regret later. Assume e-mails are never erased.

- Add a confidentiality message footer to your messages, such as: CONFIDENTIALITY NOTICE: This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.

If you receive e-mail with unencrypted confidential information, contact the sender immediately and make them aware of your concern. Do not extend the breach of information by forwarding the e-mail to others.

If you are notified that you sent an e-mail with PHI to the wrong recipient, request that the recipient destroy all copies and refrain from forwarding the information. Immediately contact the Privacy Officer for next steps.

Fax

- Never fax PHI to an unsecured fax machine. (A secure fax is one located in a restricted environment.) Call ahead to ensure that the intended recipient will pick up the fax.

- Always check the destination fax number before faxing.

- Use cover sheets containing a confidentiality statement, such as: CONFIDENTIALITY NOTICE: This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.

- Return items which you have received in error (faxed to the wrong location or improperly faxed) and advise the sender of the error.

- If you are advised that you sent a fax of PHI to the wrong number, confirm that the recipient destroyed all copies and did not share the information. Immediately contact the Privacy Officer for next steps.

Voice Mail/Answering Machines/Telephone Communication

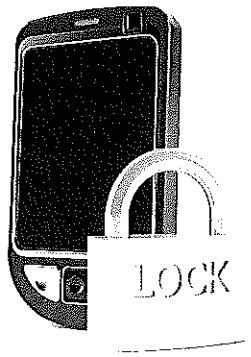
- Consider who has access to your voice mail or answering machine so others do not access that PHI.

- Be careful about what messages you leave on answering machines and voice mail.

- If you use a speaker phone, be aware of your surroundings and sensitive to the messages being replayed.

- If you are advised that you left PHI on the wrong voice mail, confirm that the recipient deleted the message and did not forward the information. Contact the Privacy Officer for next steps.

Mobile Computing Devices and PDA's



A mobile computing device includes all devices/media capable of storing and/or transmitting data in an electronic format. These devices include, but are not limited to, laptops, PDAs, cell phones, Bluetooth devices, memory sticks/thumb drives, external hard drives and digital cameras.

- Do not download or store PHI or other confidential information on mobile devices.

- Never leave devices in an exposed or unsecured area.

- Always password-protect mobile devices.

- Utilize physical locks for laptops and other mobile devices.

- Keep mobile devices up-to-date with current operating system security patches.

- Ensure that mobile devices are compliant with CKHS minimum security standards.

- Off-site work requires greater vigilance to maintain the required level of privacy and security. Offsite workers may access CKHS systems via approved, secure remote access methods only.

- Be alert to recognize and report all privacy and security incidents to your department supervisor or manager, the Compliance

Helpline (1-800-387-7921) or the CKHS Privacy Officer.

- Immediately report lost or stolen devices to the CKHS Security Department.
- Never text PHI or redirect CKHS email to your PDA.

Guidelines for Professional Participation in Social Media

When you participate in social media platforms, such as Facebook:

- Never post any information that can be used to identify a patient or a patient's condition in any way.
- Respect copyrights and trademarks, and protect and do not disclose proprietary financial, intellectual property, patient care or similar sensitive or private content.
- Make it clear when you are not speaking as an official representative of CKHS, and that you are expressing your personal views and opinions, which are not necessarily the views and opinions of CKHS.
- Individuals who identify themselves as associated with CKHS in communications on social media platforms must communicate in ways that reflect favorably upon their CKHS colleagues, leaders and even CKHS patients and donors.
- Post meaningful, respectful comments and refrain from remarks that are off-topic and offensive. Remember that all content contributed on social media platforms becomes immediately searchable and leaves the participating individual's control forever.
- If someone from the news media contacts you about posts made on social media platforms that relate to CKHS , you must alert the Vice President of Marketing before responding.

- Failure to follow these guidelines may result in disciplinary action up to and including termination of employment.

Other Federal Laws

In addition to HIPAA, there are other federal laws which govern the release of information, mandate that information be protected, and in some cases require that individuals be granted certain rights relative to control of and access of their information.

The Federal Trade Commission charged with protecting consumers requires banking and other industries to implement "red flag" standards (12 CFR Part 681) to detect and prevent identity theft related to customer and service accounts. These red flag rules extend to health care institutions.

The Family Education Rights and Privacy Act (FERPA) governs the protection of education records which include student health records (20 USC 1232g). HIPAA specifically exempts individually identifiable health information in education records. As FERPA records are exempt from HIPAA, all releases from education records must be in accordance with FERPA regulations.

Federal Department of Health and Human Services as well as other federal agencies require the protection of the privacy and confidentiality of participants in research clinical trials.

Frequently Asked Questions (FAQs)

There has been a breach of patient privacy in my department. What do I do?

If the personally identifiable information was on a stolen device (computer, PDA, for example), immediately contact CKHS Security Department to report the theft and if personal health information is involved, contact the Privacy Officer. The CKHS Security Department will contact IS. For disclosures not involving a stolen device, contact the Privacy Officer immediately.

In every circumstance, you will need to provide the following information:

- Date and time breach was discovered
- Name of and contact information for person who discovered breach
- The specific patient information disclosed
- The number of patients who had their information disclosed
- How it happened
- Actions taken following detection
- The department contact for follow-up

The Privacy Officer will responsible for investigating the breach; communicating with patients; and determining and implementing corrective steps and changes in process.

How do we handle vendors who come into a CKHS Hospital?

Before allowing vendors access to a CKHS hospital, they need to check in with Materials Management. Once this is complete, they must wear a Visitor ID at all times while in the CKHS facility. Do not leave vendors alone in areas with PHI that they do not need to have access to i.e., patient care areas.

How can I leave a HIPAA compliant telephone message with someone or a voice mail?

Leave the minimum amount of information needed: your name, phone number and that you are from CKHS.

What patient information may be faxed?

You may fax only the minimum information necessary. Best practice is to confirm the correct fax number prior to sending, include a cover letter with a confidentiality statement and call to confirm receipt.

May I mail my patient's information?

If you have a patient care need to do so, yes. Best practice is to confirm the correct address with the patient prior to sending and make sure it does not have any other identifying information on the outside, other than CKHS.

For white boards or marker boards, what information may be listed?

The use of last names and first initials on the board within the department is appropriate. In the operating room, first and last names are permitted for safety reasons. The important considerations are: whether the board is visible to passers-by and whether it contains PHI. If yes to both, consider whether there are other ways that the protected data (including demographic data) could be "reasonably" limited to the minimum necessary to allow the unit to safely manage patient care.

Frequently Asked Questions (FAQs)

There has been a breach of patient privacy in my department. What do I do?

If the personally identifiable information was on a stolen device (computer, PDA, for example), immediately contact CKHS Security Department to report the theft and if personal health information is involved, contact the Privacy Officer. The CKHS Security Department will contact IS. For disclosures not involving a stolen device, contact the Privacy Officer immediately.

In every circumstance, you will need to provide the following information:

- Date and time breach was discovered
- Name of and contact information for person who discovered breach
- The specific patient information disclosed
- The number of patients who had their information disclosed
- How it happened
- Actions taken following detection
- The department contact for follow-up

The Privacy Officer will responsible for investigating the breach; communicating with patients; and determining and implementing corrective steps and changes in process.

How do we handle vendors who come into a CKHS Hospital?

Before allowing vendors access to a CKHS hospital, they need to check in with Materials Management. Once this is complete, they must wear a Visitor ID at all times while in the CKHS facility. Do not leave vendors alone in areas with PHI that they do not need to have access to i.e., patient care areas.

How can I leave a HIPAA compliant telephone message with someone or a voice mail?

Leave the minimum amount of information needed: your name, phone number and that you are from CKHS.

What patient information may be faxed?

You may fax only the minimum information necessary. Best practice is to confirm the correct fax number prior to sending, include a cover letter with a confidentiality statement and call to confirm receipt.

May I mail my patient's information?

If you have a patient care need to do so, yes. Best practice is to confirm the correct address with the patient prior to sending and make sure it does not have any other identifying information on the outside, other than CKHS.

For white boards or marker boards, what information may be listed?

The use of last names and first initials on the board within the department is appropriate. In the operating room, first and last names are permitted for safety reasons. The important considerations are: whether the board is visible to passers-by and whether it contains PHI. If yes to both, consider whether there are other ways that the protected data (including demographic data) could be "reasonably" limited to the minimum necessary to allow the unit to safely manage patient care.

Questions or Comments

If you have any questions about the CKHS Privacy and Information Security policies, you are encouraged to talk to your supervisor or another member of management. If, however, your question or concern cannot be resolved through these channels, you should contact the CKHS Privacy Officer directly or though the Compliance helpline (1-800-387-7921).

Non-Retribution Policy

CKHS will not take any disciplinary action or other types of retaliation against any employee who, in good faith, reports a privacy or information security concern to management, the Privacy Officer or the Employee Helpline. "Good faith" does not mean that you have to be right – but it does mean that you should be telling the truth as your know it.

Any employee who believes that he or she has suffered retaliation from making a report should contact CKHS's Privacy Officer or Employee Helpline.

In contrast to a good faith report, intentionally making a false accusation is a serious violation of policy and may lead to disciplinary action up to and including termination of employment.

Violation of Law, Regulation or the Code

CKHS attaches the utmost importance to obeying the law and conducting business professionally and ethically. Any employee, regardless of their position or length of service, who engages in, causes, or by their inaction or inattention fails to detect, tolerates or condones any form of illegal or unethical conduct has violated the Code of Conduct and is subject to immediate disciplinary action, up to and including, termination of employment.

NOTES

Crozer-Keystone Health System Members

Crozer-Chester Medical Center ~ *Upland*
Crozer Medical Plaza at Brinton Lake ~ *Glen Mills*
Delaware County Memorial Hospital ~ *Drexel Hill*
The Physicians of Crozer-Keystone ~ *Springfield*
Media Medical Plaza ~ *Media*
Springfield Hospital ~ *Springfield*
Taylor Hospital ~ *Ridley Park*
Community Hospital ~ *Chester*

CROZER-KEYSTONE
HEALTH SYSTEM

We're 5 hospitals, 2,600 doctors and nurses,
and 6,800 caring people with 1 vision.
Crozer-Keystone. Something to feel good about.