Holyoke Hospital, Inc.

INTRODUCTION TO HOLYOKE HOSPITAL'S CORPORATE COMPLIANCE PROGRAM

DEPARTMENT OF EDUCATION AND TRAINING

INTRODUCTION

Holyoke Hospital's Corporate Compliance Program is a vital component to helping us maintain our reputation with our patients and the community as an honest and efficient provider of quality health care. This program assures that we conduct our work in a way that is compliant with laws and regulations and is consistent with our ethical code of behavior. Adherence to the spirit of the program is essential to the hospital's future.

This booklet is an introduction to the basic elements of the Hospital's program. Depending on where you work, you will receive more specific education about the hospital's plan from your Department Manager/ Supervisor. Employees are always encouraged to refer to the entire Corporate Compliance manual (available on your unit) for further information/clarification.

The policies described in this booklet are mandatory and must be followed by all staff, regardless of position, as a condition of employment. This program applies to employees, contracted personnel, medical staff, volunteers, students and other agents. Each and every individual has a responsibility to be familiar with the laws and regulations that apply to his or her duties and responsibilities and to conduct themselves accordingly.

Read through the entire booklet, complete the exercise, and fill-out and return the acknowledgment form.

If you have any questions or comments about our Compliance Program, feel free to contact the Compliance Officer or your Department Manager at any time.

The hospital is here to support you as we work together to do the right thing.

HOLYOKE HEADLINES

"OFFICE OF THE INSPECTOR GENERAL STIPULATES THAT EVERY HEALTH CARE ORGANIZATION DEVELOP A CORPORATE COMPLIANCE PROGRAM....."

WHAT IS A CORPORATE COMPLIANCE PROGRAM ??

A corporate compliance program is designed to ensure that our hospital continues to **conduct itself in a manner that is ethical and consistent with good business practices**.

WHY DO WE NEED A PLAN?

We all know that doing business in today's environment isn't always easy. The healthcare industry is faced with increased scrutiny by the government and private insurers. Our actions are evaluated daily by our community and patients. Those organizations who chose to violate regulatory and ethical standards face multi-million dollar fines, prison sentences for employees, loss of business, and loss of public trust.

Because we are all under a new level of review, we have to continue in our good faith effort

" TO DO THINGS RIGHT
AND
DO THE RIGHT THINGS".

Our Corporate Compliance Program gives us standards and policies that direct our actions in this challenging environment.

WHAT DOES THE PROGRAM INCLUDE?

The Compliance program includes:

WRITTEN STANDARDS OF CONDUCT

The Code of Ethical Behavior describes expectations of how we as health care workers should behave with our patients, community, and each other.

HOSPITAL POLICY STATEMENTS AND STANDARDS ON CONDUCT AND COMPLIANCE

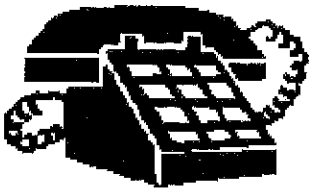
The hospital has developed expectations, standards, policies and values as they relate to workplace ethics and compliance. The policies and procedures included in the corporate compliance manual are mandatory. Each employee, regardless of position, is required to follow these policies as a condition of their employment.

EDUCATION TO TEACH STAFF ABOUT COMPLIANCE

The hospital will provide education about the standards, policies, and conduct when new employees are hired and annually thereafter. Please remember that it is the personal responsibility of all employees to learn about the laws, regulations and policies that are applicable to the jobs they perform and to conduct themselves accordingly.

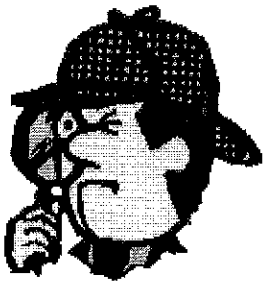
RESOURCES TO SUPPORT STAFF WHEN THEY NEED GUIDANCE ON ETHICAL AND COMPLIANCE CONCERNS OR WISH TO REPORT A VIOLATION

If you had a question about workplace conduct or saw something that you thought was wrong, there are several resources to turn to with such concerns. We first encourage you to **talk with your supervisor**. However, if for any reason you do not feel comfortable talking to your supervisor or if your supervisor did not answer the question or address the problem to your satisfaction, you do have other options.



A Compliance Phone Line can be used when you need advice or want to report a complaint or misconduct. The phone line protects the informant's identity/anonymity.

There is also a person in charge of our corporate compliance program called a **compliance officer**. His job is to develop and oversee the compliance program. Our Corporate Compliance Officer is Clark Fenn. He is also available to assist staff and management in developing our skills to recognize and resolve work related ethics and compliance concerns. Finally, you may also contact **Human Resources** or a **member of the compliance committee**.



COMPLIANCE OFFICER

Regardless of how or from whom you seek support and guidance, it is important to remember that each individual has an obligation to resolve and report concerns regarding actual or potential ethical or compliance violations. While it may seem easier to look the other way and not get involved, please remember that when faced with and ethical or compliance issues . . . . .

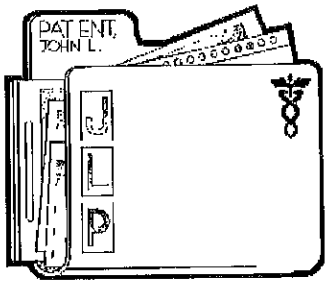
SILENCE DOES NOT DEMONSTRATE INTEGRITY.

HOW DO I RECOGNIZE POTENTIAL ETHICAL AND COMPLIANCE CONCERNS?

Potential conduct and compliance violations can occur in such areas as. .

✔ **PATIENT INFORMATION & CONFIDENTIALITY**
Employees have access to confidential information concerning the hospital, our patients and other employees and members of the medical staff. Safeguarding confidential information is essential to the conduct of our business. To ensure confidentiality of hospital information, we must adhere to our confidentiality policy.

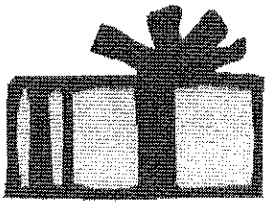
✔ **ACCURATE RECORDS/NOT TAMPERING WITH RECORDS**

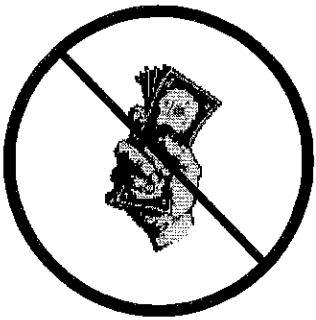


Our responsibility is to provide accurate and responsible information in the medical record. That means never tampering with records by going back and adding information to cover up a mistake, committing fraud by falsifying dates , entries, or signatures.

✔ **IMPROPER GIFTS TO EMPLOYEES**

As a matter of policy, employees should not accept a gift or payment for an activity of more than a token value from any individual or organization with whom the hospital does business, has done business, or who is seeking to do business with the hospital. Nominal promotional items such as pens, calculators, etc., are examples of token items.





REGARDLESS OF THE AMOUNT, CASH GIFTS OR GIFT CERTIFICATES SHOULD NEVER BE ACCEPTED.

✔ **FALSIFYING CODING IN MEDICAL RECORDS OR FINANCIAL RECORDS**

Under no circumstances should records be back-dated, intentionally destroyed or tampered with. All bills rendered to the patient, their representatives or third parties must accurately reflect the services rendered, and all business records, vouchers, and payroll records are to be prepared with care and honesty. No one may make or order another person to make false or misleading entries into books or records of the hospital.

✔ **VIOLATION OF WORKPLACE CONDUCT**

Many employee policies have been created and maintained in accordance with applicable federal, state and municipal laws and regulations. For example, sexual harassment violates a federal law and is a reportable compliance issue. Employees are responsible for following the spirit of the sexual harassment policy.

QUESTIONS AND ANSWERS

The following are some real life examples of ethical and compliance concerns that you may face in your daily work. Before reading the responses, use this 3 C Decision Making Model.

First ask yourself....

COMPLIANCE
"Does this situation involve a violation of a law, regulation, internal policy or procedure?"

CONSCIENCE
"Does this situation involve violating an ethical principle?"

If the answer is yes to one or both, then ask yourself...

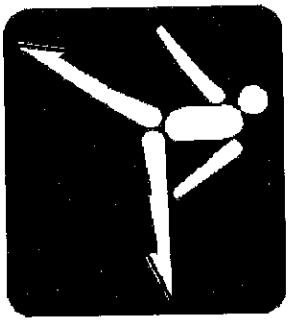
CONDUCT
"What are my alternatives for addressing this situation and what actions should I take and when?"

Read through each of the following situations using this 3 C Decision Making Model. This will help you gain a better understanding of our commitment to integrity in all our interactions and workplace conduct.

What should I do if my supervisor asks me to do something I think violates the Hospital's Code of Ethical Behavior or is illegal?

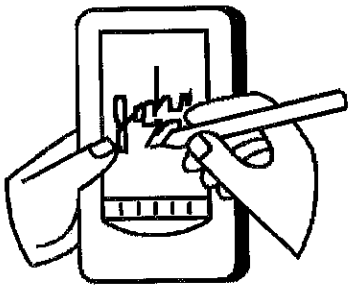
Do not do it. No matter who asks you to do something, if you know it is wrong, you must refuse to do it. You must also immediately report the request to a level of management about your supervisor or to the Corporate Compliance Officer.

How do I know if I am on ethical "thin ice"?

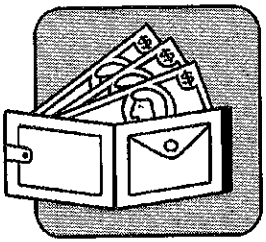


If you are worried about whether your actions will be discovered, if you feel a sense of uneasiness about what you are doing, or if you are rationalizing your activities on any basis (such as perhaps the belief that "everyone does it"), you are probably on ethical "thin ice". Stop, step back, consider what you are doing, get advice from the compliance officer, and redirect your actions to where you know you are doing the right thing.

In preparation for an accreditation visit, my supervisor has asked to review medical records and to fill in any missing signatures. May I do this?

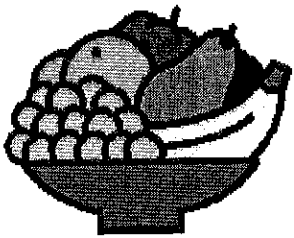


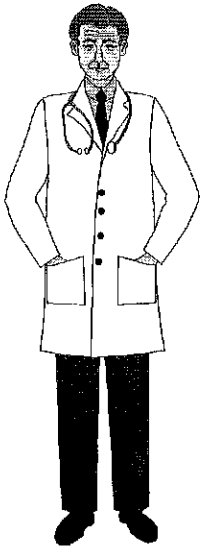
No. It is absolutely wrong to sign another healthcare provider's name in the medical record. It is part of our basic integrity obligation to provide accurate and responsible information to accrediting groups.



A patient with a chronic health condition is frequently admitted to our facility for *treatment. He routinely tips his primary nurse around $40. May the nurse accept it?*
No. Cash gifts must never be accepted from anyone with whom we have a business relationship.

May a Department or individual accept a basket of fruit or flowers that a patient sent?
Yes. Gifts to an entire department or an individual may be accepted if they are consumable or perishable.





We live in a small town and most of the community knows each other. There is a physician in our hospital who sometimes requests medical records, whether he is taking care of the patient or not. Is he allowed to do this?

No. Only the attending, covering, or consulting physician may have access to the patient medical record. We are responsible for protecting the confidentiality of patient information from interested third parties as well as our staff. Patients are entitled to expect confidentiality, the protection of their privacy and the release of information only to authorized parties.

Do the conflict of interest policies apply to distant relatives, such as cousins or in-laws or friends?

The conflict of interest policies generally apply to members of your immediate family. However, if any relationship could influence your objectivity or create the appearance of impropriety, you must apply the policies.

If I report something suspicious, will I get into trouble if my suspicions turn out to be wrong?

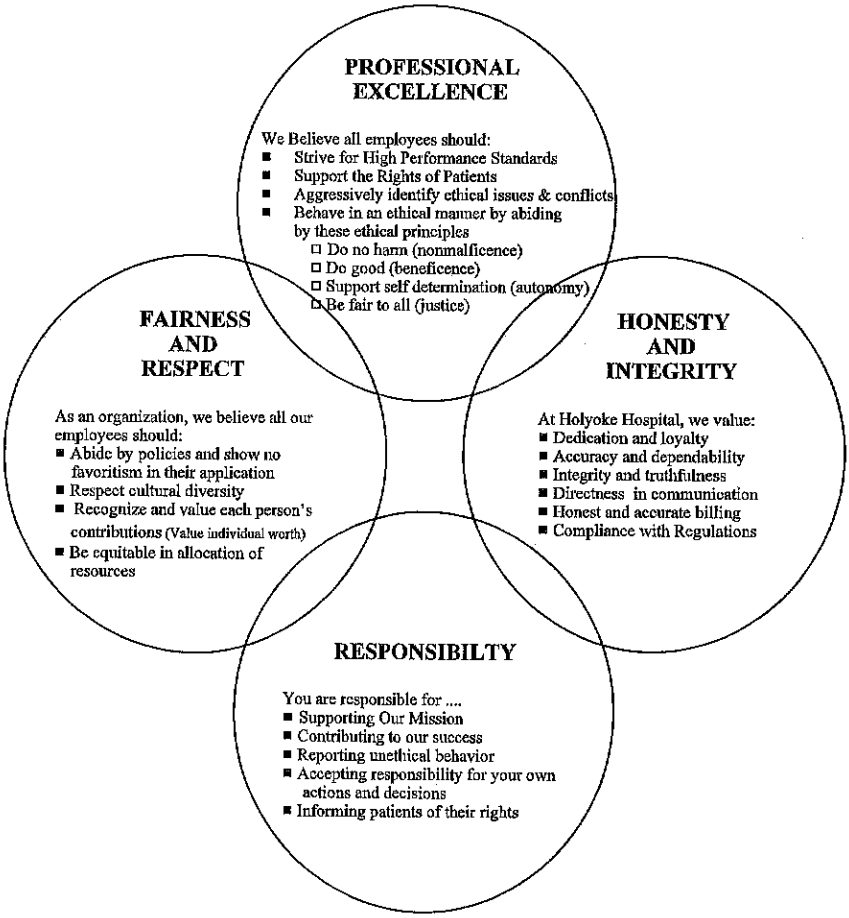
As long as you honestly have a concern, Hospital policy prohibits your being reprimanded or disciplined. As a hospital employee, you have the responsibility to report suspicious problems. In fact, employees any be subject to discipline if they witness something but do not report it. The only time someone will be disciplined for reporting misconduct if she or he knowingly and intentionally reports something that he or she knows to be false or misleading in order to harm someone else.

CODE OF ETHICAL BEHAVIOR

This code outlines four values and service principles that should guide our conduct/ behavior/actions as employees of the hospital. If we follow these guidelines, we commit to providing the best possible experience for our patients, families, other clients as well as for our coworkers.

HOLYOKE HOSPITAL'S CODE OF ETHICAL BEHAVIOR

4 CORE VALUES



SUMMARY

Remember, we are all committed to ethics and compliance in our daily decision making and conduct. Your adherence to the Corporate Compliance program is essential to the future of our hospital. When we conduct our day to day work in compliance with the program, we will be serving the MISSION of Holyoke Hospital, Inc. to serve the health needs of the community in a compassionate, high quality, and efficient manner.

To call for guidance or to report a violation,
call our

HEALTHCARE VALUES PHONE LINE
1-800-273-8452

or call our

Corporate Compliance Officer

Clark Fenn, VP Management Services	534-2584

or call a member of the

Compliance Committee. . . .

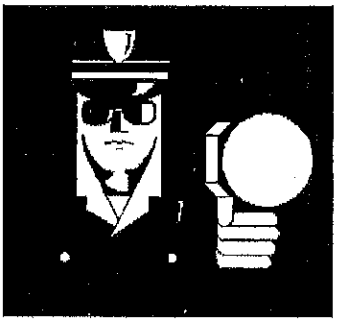
Hank Porten, President	534-2554
William Andrews, COO	534-2554
Margaret Barry, VP Behavioral Health	534-2617
Tony Correia, Corporate VP Finance	534-2554
Paul Silva, VP Finance	534-2554
Mary Kelleher, VP, Human Resources	534-2547
Kathy Buckley, VP Marketing	534-2520
Sarah King, VP Nursing	534-2510
Mike Zwirko, VP Operations	534-2554
Garry Bombardier, MD, Medical Director	534-2578
David Wilbur, Director of Planning	534-2572

12/99; 3/220: F:\DATA\WP\EDUC\Private\JOYANN\CORPORATE COMPLIANCE\CORPORATECOMPLIANCETRAININGBOOKLET.wpd

HOLYOKE MEDICAL CENTER

HIPAA TRAINING:

INFORMATION SECURITY



"Information Security is Everyone's Business"

COPRPORATE COMPLIANCE DEPARTMENT

INFORMATION SECURITY RESOURCES:

Telephone Numbers:

Information Security Officer	534-2741
Privacy Officer	534-2534
Risk Management	534-2584
Corporate Compliance Manager	534-2500 x5615
Information Systems Help Desk	534-2500 x5294

Policies & Procedures:

Administrative Policy Manual
- Information Management
  - Privacy
  - Security

Department Specific Policy and Procedure Manual

Personnel Policy Manual

Regulations:

Federal: 45 CFR 160, 162 and 164: Health Information Reform, Security Standards.

INTRODUCTION

Information security is required to maintain the confidentiality, integrity and availability of Holyoke Medical Center's information systems.

The information provided in this training handbook introduces you to the Health Insurance Portability and Accountability Act (HIPAA) which resulted in several rules, one of which is the security rule. The HIPAA Security rule goes into effect on April 20, 2005 and is the first federal regulation to mandate security standards to protect patient health information (PHI).

The policies and procedures described in this handbook are mandatory and must be followed by the entire hospital workforce, regardless of position, as a condition of employment. These security standards also apply to contracted personnel, medical staff, volunteers, students and other agents. Each of us has a responsibility to become familiar with the policies and procedures that apply to information security and to maintain a high level of awareness.

This training reflects the standards, policies and procedures that we must follow to maintain information security.

Upon completion of this training you will:

- Have a basic understanding of HIPAA Security regulations
- Understand good information security procedures
- Know where to find the policies and procedures
- Know where to refer issues, concerns and questions regarding information security

Please read through this entire handbook, complete the challenge questions, fill out and return the acknowledgment form.

If you have any questions or concerns about information security, feel free to contact the Information Security Officer or your Department Manager.

HIPAA INFORMATION SECURITY OVERVIEW

HIPAA, which stands for the Health Insurance Portability and Accountability Act, is a federal law enacted with the goal of improving the continuation of health insurance coverage to make it easier for people who change health insurance plans as a result of changing jobs or becoming unemployed. However, the law also included a number of standards designed to protect patient information and to standardize billing and other areas of health information.

Today, almost all patient information is stored and transmitted electronically. The security standards were developed to protect that patient information.

Privacy and Security go hand-in-hand. Where the HIPAA Privacy Rule deals with "How data is disclosed" and "To whom data is disclosed", the HIPAA security rule deals with "How data is stored" and "How data is accessed". Without security there is no privacy.

The security standard consists of three major sections:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Each of the sections consists of various standards. Each standard is designed to protect the confidentiality, integrity and availability of patient information. The table below shows the three categories and a few of the standards for each:

Administrative Safeguards	Physical Safeguards	Technical Safeguards
Risk Analysis & Management - Identify, Evaluate, Reduce & Control	Facility Access Controls - Door Locks, Video Surveillance, Access Logs	Access Controls - Passwords, Terminations, Access Rights
Security Awareness & Training - Initial Training - Annual Retraining	Workstation Uses & Controls - Auto logout - Screen Savers	Auditing Controls - Access Verification, Equipment
Contingency Plan - Disaster Recovery - Downtime Procedures	Device & Media Controls - Disposal Media - Backups	Transmission Security - Encryption - Wireless

The HIPAA Security regulations apply to the hospital's entire workforce. That includes senior management, department managers, supervisors, employees, volunteers, students, instructors, doctors, vendors and consultants. It doesn't matter if they are full time, part time or only Per Diem. It makes no difference if they have access to patient information or not. Everyone at Holyoke Medical Center must comply with the HIPAA security regulations.

HIPAA SECURITY TRAINING OVERVIEW

HIPAA mandates that the entire workforce receive initial HIPAA security training, periodic reviews, as well as regular reminders and awareness reinforcement. Areas of security that the workforce must receive training in include:

- Basic Security Behaviors
- Password Management
- Protection From Malicious Software
- Workstation Security
- Login Monitoring
- Awareness Training
- Incident Reporting Procedures

BASIC SECURITY BEHAVIORS

There are some very basic behaviors to maintain information security that you must be aware of in your day to day activities:

- Limit viewing of PHI to your job function, even if you can accidentally see other information
- Any information seen on someone's desk or computer monitor is private and should be kept that way
- Ensure PHI is not viewable by visitors or patients
- Any information, not your own, is not to be discussed, even if accidentally viewed
- Dispose of materials containing PHI properly
- Never share network logins or passwords
- Report any compromises or losses to your Supervisor or the Information Security Officer
- Ensure good physical security
  - Lock doors
  - Don't leave laptops, PDAs or other portable devices unattended
  - Be aware of strangers in your area
- Logoff or lock workstation when not in use

PASSWORD MANAGEMENT

Passwords are the hospital's first and best line of defense to protect its information systems. They provide access only to those functions and information that you need to do your job. Your password identifies you. It is your computer "Signature." Protect your password as carefully as you do your own signature and never disclose or share your password with anyone, not even your department manager. Don't write your password down.

Holyoke Medical Center has established the following standards for passwords to its information systems:

- A User ID is required in addition to the password
- Passwords must be a minimum of 6 characters in length
- Passwords must be changed every 60 days
- Passwords can only be used once
- Passwords can't be easy to guess

There are several techniques available to help you remember passwords at the same time picking a password that is hard to guess.

- Passwords that use the same base word but add characters and numbers to it. The characters and numbers are changed every 60 days but not the base word. Examples are:

DRIFT	4DRIFTP8
PUTTY	79FPUTTY
KREPS	KREPS52B

- Passwords which combine parts of 2 or more things you know. Examples are:

Red Sox & Fenway Park	REDFENWAY
TV Show on NBC called ER	SHOWNBCER

- Passwords that utilize parts from a line/title from songs, books, TV, movies, etc:
  - MOONRIVER
  - AMERIDOL
  - CHICKENROAD
  - DOUFEELLUCKY

PROTECTION FROM MALICIOUS SOFTWARE

Each and every day new versions of malicious software try to attack the hospital's information systems. The purpose of this software is to cause havoc of some type. They can cause anything from an annoyance to complete destruction and loss of all hospital software.

Malicious software comes in the form of computer viruses, worms or trojans. It's important that you do all you can to protect the hospital's information systems from this type of software. Follow these rules:

- Never download software from the Internet
- Never install any software applications without approval from Information Systems
- Never install screen savers and weather bugs
- Never install peer-to-peer software (Kazaa, Napster)
- Never use Instant Messaging
- Never utilize Internet Radio services
- Shut off computer and monitor when leaving for the day
- Use only Holyoke Medical Center mail systems (No Hotmail, Yahoo, etc)
- Only read an email message that passes each of the following tests:

Know test: Is the mail from someone that you know?
Received test: Have you received email from the sender before?
Expect test: Were you expecting email with an attachment?
Sense test: Does the email from the sender have contents as decribed in the subject line and the attachment name make sense?
Virus test: Does the email contain a virus? Use antivirus programs.
IF THE EMAIL DOESN'T PASS ALL 5 TESTS "DELETE IT"!

The hospital utilizes GroupWise for its email software.

- GroupWise email does not utilize encryption for external mail
- Account number or a medical record number, can only be utilized for internal email. External email with PHI is **NOT** allowed.
- The use of all other PHI information is prohibited
- The automatic forwarding of GroupWise email to an external account is prohibited

Holyoke Medical Center runs virus protection software on every workstation. The virus software is active when you see a small icon on the right side of your Windows Taskbar that looks like an EKG Reading.

If the virus software icon isn't present on your Taskbar or is inactive (circled in red and crossed out) you must notify the Information Systems Help Desk at x5294 immediately.

WORKSTATION SECURITY

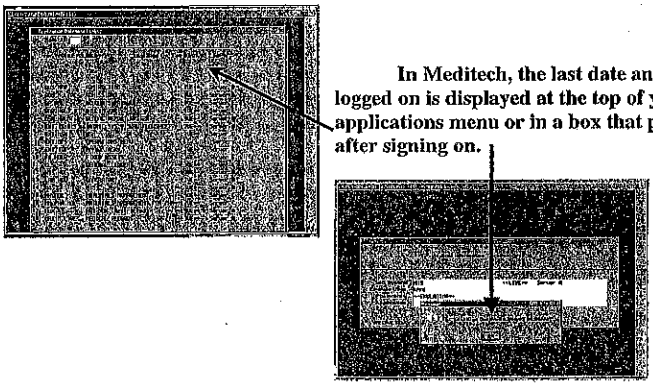
There are a number of steps each of us must follow to maintain a high level of security for our workstations.

- Never use someone else's password to login
- Never use a workstation under someone else's login
- Always shutdown your workstation and monitor at the end of each day.
- Keep the monitor from view of visitors and patients
- Do not lookup information you don't need to do your job. That includes information for a friend, family member, colleague or even yourself.
- Do not leave a workstation logged in and not locked.
  - > The password screensaver is only a precaution.
  - > When leaving your workstation you should always logout or lock it by entering <*Ctrl*> + <*Alt*> + <*Delete*> keys, followed by an <Enter> to lock the workstation.

LOGIN MONITORING

As a deterrent to unauthorized access, the hospital disables access after 6 consecutive invalid login attempts. You must call the Information Systems Help Desk at x5294 to have your access unlocked. Outside normal business hours nursing departments should notify the Clinical Supervisor, all other departments should notify the Information Systems on-call person.

At the time you login, some systems like Meditech show the last date and time you logged on. You should always verify that it is correct. You know there is a problem if it indicates you logged in yesterday and you returned today from a week off. Notify your manager or the Information Security Officer if it's wrong.



In Meditech, the last date and time you logged on is displayed at the top of your applications menu or in a box that pops up after signing on.

HIPAA Training: INFORMATION SECURITY

AWARENESS TRAINING

It's important to have information security awareness in everything you do at the hospital. We all have a responsibility to maintain patient privacy and protect patient information. It's the right thing to do and it's the LAW. There are many things you can do to maintain information security, here are just a few:

- Is the patient information on the printer, monitor, fax machine, whiteboard safe from unauthorized eyes?
- Is the trash with the patient's name on it in the right container for shredding?
- Does that person belong here?
- Does your last login date and time look correct?
- Did I lock my workstation as I walked away?
- Does that person really have a "need to know"?

INCIDENT REPORTING PROCEDURES

If you witness or suspect an information security issue or violation, no matter how small you have a responsibility to report it. Notify one of the following individuals as soon as possible:

- Your supervisor
- Your manager
- Information Security Officer
  - Outside normal business hours nursing departments should notify the Clinical Supervisor
  - All other departments should contact the Information Systems on-call person

ENFORCEMENT

HIPAA security is the law. Failure to comply with the regulations of HIPAA security can result in significant civil and criminal penalties.

- Civil penalties
  - $100 per day, per violation
  - maximum of $25,000 annually
- Criminal penalties
  - $50,000 and/or imprisonment for up to 1 year for any person who knowingly obtains and discloses PHI
  - $100,000 and/or imprisonment for up to 5 years if under false pretenses
  - $250,000 and/or imprisonment for up to 10 years if intent to sell information

SUMMARY

This handbook has taught you what you need to do to maintain a high level of information security and protect the hospital's information systems. Keeping patient information confidential and available must be a goal for each of us.

The Holyoke Medical Center's Information Security policies and procedures can be found within the Information Management's section of the hospital's Administrative Policy Manual.

If you have any questions about this handbook, please contact the Information Security Officer at 534-2741.

Please remember "***Information Security is Everyone's Business***".

Holyoke Medical Center

CHAPTER: Management of Information	**POLICY # A10-127**
SUBJECT: Privacy: Red Flags Identity Theft Prevention Program	**Page 1 of 5**
Date Initiated: 4/9/2009	**Date Reviewed/Revised: 10/2010**
Distribution: ALL HOLDERS OF ADMINISTRATIVE POLICY MANUAL	

A POLICY

It is the policy of Holyoke Medical Center (HMC) to have a Red Flag Identity Theft Program in place that will detect, prevent, and mitigate identity theft in connection with all hospital covered accounts.

B PURPOSE

The purpose of this program is to:

1. Comply with the Federal Trade Commission (FTC) Red Flag Regulations
2. Identify the relevant Red Flags based on risk factors associated with the hospital's covered accounts.
3. Establish policies and procedures for detecting Red Flags for Identity Theft.
4. Identify steps the hospital will take to prevent and mitigate Identity Theft.
5. Create a system for regular updates and administrative oversight to the program.
6. Develop a training program that educates and creates awareness for hospital staff to identify and mitigate Identity Theft.

C PROCEDURES

1. The Identity Theft Red Flags Mitigation and Resolution Procedures (Attachment A) identify the Red Flags that have been determined to be the most relevant for the hospital.
   a. Red Flags generally fall within one of the following general types:
      1. Suspicious documents
      2. Suspicious personal identifying information
      3. Suspicious or unusual use of a covered account
      4. Alerts from outside the hospital, such as a patient, law enforcement or an identity theft victim.

2. Preventing and Mitigating Identity Theft
   a. The Meditech system's Verify Information Personally (VIP) function will be utilized to flag an account with a Red Flag. "VIP" Flagging: also known as "flagging" the account is instituted when a client has been identified as a known or potential victim of Identity Theft. The VIP process consists of the following:
      1. The staff person who identifies an issue that warrants VIP flagging notifies the Patient Registration Manager by email. The email must contain the client's medical record number, name, and reason to red flag the account or status after acting on an existing Red flag.

2. Only the Patient Registration Manager may activate or deactivate the VIP flag.
3. If the Patient Registration Manager questions the staff person's assessment of the situation to "flag" the account , the manager can notify the hospital's Regulations Committee to review the situation.

b. Specific action steps to prevent, mitigate, and resolve each Identity Theft Red Flag are listed in the attached Identity Theft Red Flags Mitigation and Resolution Grid (Attachment A).

3. Detection of Red Flags
   a. All employees who have contact with a client's financial, demographic, or medical information are in a position to potentially detect Identity Theft Red Flags as defined in the attached Identity Theft Red Flag Mitigation and Resolution Grid.

4. Program Administration
   a. The Regulations Committee is responsible for developing, implementing, administering, and updating the Red Flag Identity Theft program including all education and training programs.
   b. The Regulations Committee will review past Red Flags and resolutions and assess any new Red Flags that have occurred.
   c. The Patient Registration Manager will be responsible for maintaining a log of all accounts that have been flagged and all Red Flag activity on those accounts. The Patient Registration Manager will report this activity to the Regulations Committee.

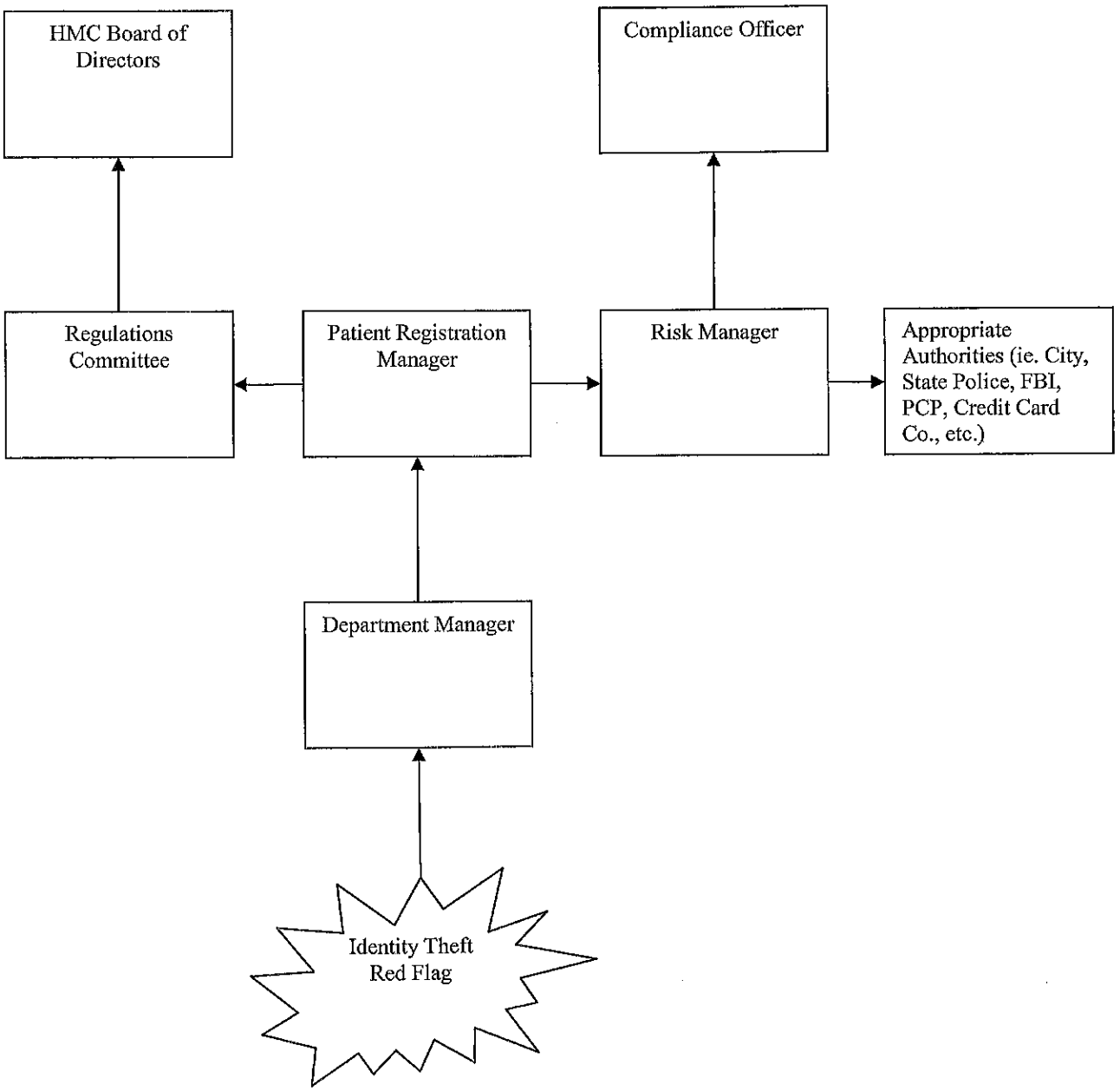
5. Training
   a. All employees of the hospital will receive initial education and training that includes general information on the hospital's Red Flag Identity Theft policy and procedures. This will include all new employees during their orientation process.
      1. Refer to the Red Flag Regulation Competency Test (Attachment B) for the hospital's general training document.
   b. All employees of the hospital will also receive annual review training as part of their Risk Management Education Review.
   c. Department specific education and training will be required on an annual basis for all departments that are directly affected by the Red Flags Identity Theft policy and procedures.

1. Department specific training must be approved by the hospital's Regulations Committee.
2. Departments that require department specific training include:
   a. All areas that register patients
   b. All areas that take credit/debit cards
   c. All areas that do patient billing
   d. All areas that do patient care
   e. All areas that maintain patient records
3. The Managers of those departments which are subject to department specific training are responsible for developing the annual review and competency test.

6. The hospital will require by contract or Business Associate Agreement that service providers who perform activities in connection with covered accounts have policies and procedures in place designed to detect, prevent, and mitigate the risk of Identity Theft with regard to the covered accounts.

7. If fraudulent activity has been reported, Risk Management will notify the appropriate law enforcement agency. This may include the Local and State Police as well as the FBI. When appropriate, additional notification will be made to primary care physicians, credit card companies, etc. The reporting process will follow the diagram below.

Red Flag Reporting Flow



D DEFINITIONS

Identity Theft	Fraud committed by the use of identifying information of another person.
Red Flag	An activity, pattern or practice that indicates the possible existence of identity theft.
Covered Accounts	Any account the hospital establishes or maintains.
Additional Documentation	Includes but not limited to the following: Drivers License, State Issued Identification Card, Military ID, Passport, Birth Certificate with seal, Social Security Card, etc.

ATTACHMENT A
IDENTITY THEFT RED FLAGS MITIGATION AND RESOLUTION PROCEDURES

IDENTITY THEFT RED FLAGS	PREVENTION/MITIGATION PROCEDURES	RESOLUTION OF RED FLAG
Unusual account activity, such as an increased number of accounts or inquiries.	Follow procedures to Red Flag the account. Indicate volume and frequency concerns.	Upon client's next visit additional documentation must be provided to resolve the Red Flag.
Documents provided for identification appear to be altered or forged.	Stop the process and require the client to provide additional satisfactory information to verify their identity.	Additional documentation must be provided to resolve discrepancy.
Photograph on ID inconsistent with appearance of client.	Stop the process and require the client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy.
Information on ID inconsistent with information provided by client.	Stop the process and require client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy.
Client alerts us that they have been a victim of identify theft or personal identifying information associated with known fraud activity.	Follow procedures to Red Flag the account. Indicate requirement for client to provide positive ID during next encounter.	Additional documentation must be provided to resolve discrepancy.
In post registration/billing processes the demographic information has been determined to have identity issues.	Follow procedures to Red Flag the account. Indicate requirement for client to provide positive ID during next encounter.	Additional documentation must be provided to resolve discrepancy.
Suspicious addresses or non-existing address or phone number supplied.	Stop the process and require client to provide satisfactory identity documentation.	Additional documentation must be provided to resolve the discrepancy.
Social Security number provided matches existing number on file for a different person.	Stop the process and require client to provide satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy.
The person opening the account unable to supply identifying information or personal information is inconsistent with information already on file.	Stop the process and require client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy.

IDENTITY THEFT RED FLAGS	PREVENTION/MITIGATION PROCEDURES	RESOLUTION OF RED FLAG
Mail sent to a client repeatedly returned as undeliverable despite ongoing account activity.	Use in-house procedures (telephone#, recent Meditech accounts, telephone directory) to obtain most recent mailing address.	Patient is found and contacted. Meditech is updated or account is turned over to a collection agency for skip tracing purposes.
Organization is notified that client is not receiving paper account statements.	Verify address with client. Confirm name is on their mailbox.	Additional documentation must be provided to resolve discrepancy.
Organization is notified that it has opened a fraudulent account for a person engaged in identity theft.	Follow the procedures to Red Flag the account. Indicate account identified as fraudulent.	If the individual returns to the organization then notify Risk Management who will notify law enforcement.
Complaint/inquiry from an individual based on receipt of - a bill for another individual - a bill for a service the patient denies receiving - a bill from a healthcare provider the patient never patronized. - a notice of Insurance - benefits (EOB) for services never received.	Follow the procedures to Red Flag the account. Indicate patient complaint.	Alert treating department and continue to investigate until resolution.
Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient (e.g. inconsistent blood type, age, race, and other physical descriptions)	Stop the encounter, notify supervisor/ administrator. Investigate, interview individuals as appropriate, review previous files for potential inaccurate records. Look for items such as blood type, age, race and other physical descriptions that may be evidence of identity theft.	Depending on the inconsistency and review of previous file, either delay/ do not open a new account/service/ encounter, or terminate services/encounter. If the results of the investigation do not indicate fraud, all contact & identifying information is re-verified with patient.
Patient unable to provide photo ID	Check if the client had been flagged as having received a copy of the hospital's policy requiring proper identification.	Client will receive one warning and a copy of the hospital's policy that non emergency hospital visits require proper identification. If client doesn't provide photo ID or 2 forms of identification on subsequent visits then registration will be denied.
Credit card signature doesn't match signature on transaction slip.	Stop the transaction and require client to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy or use of the credit card is denied.