HEALTH INFORMATION MANAGEMENT (HIM)

HEALTH INFORMATION MANAGEMENT

OUTLINE:

- History
- HIPAA in a nutshell
- HIPAA basics
- Privacy Rule
- Security Rule
- PHI
- 18 PHI Identifiers
- Minimum necessary standards
- Permitted use and disclosures
- Incidental use and disclosure
- ID Badge
- MISH Notice of Privacy Practices
- HIPAA Don't's
- Protecting PHI
- PHI and Computers
- HIPAA Myths
- HIPAA violation examples
- Patient Rights

HIPAA

WHAT IS IT?

Health Insurance Portability and Accountability Act of 1996

- Is a federal law imposed on all healthcare organizations including hospitals, physician offices, home health agencies, nursing homes and other health care providers, as well as health insurance plans and clearinghouses, that protects patient health information.

SecureWorks

A Brief History of Healthcare Security Regulation

Before HIPAA, there was no universally recognized security standard or basic mandates for Protected Health Information (PHI).

The goal of HIPAA was to protect patients' confidentiality while enabling healthcare organizations to pursue initiatives that furthered innovation and patient care.

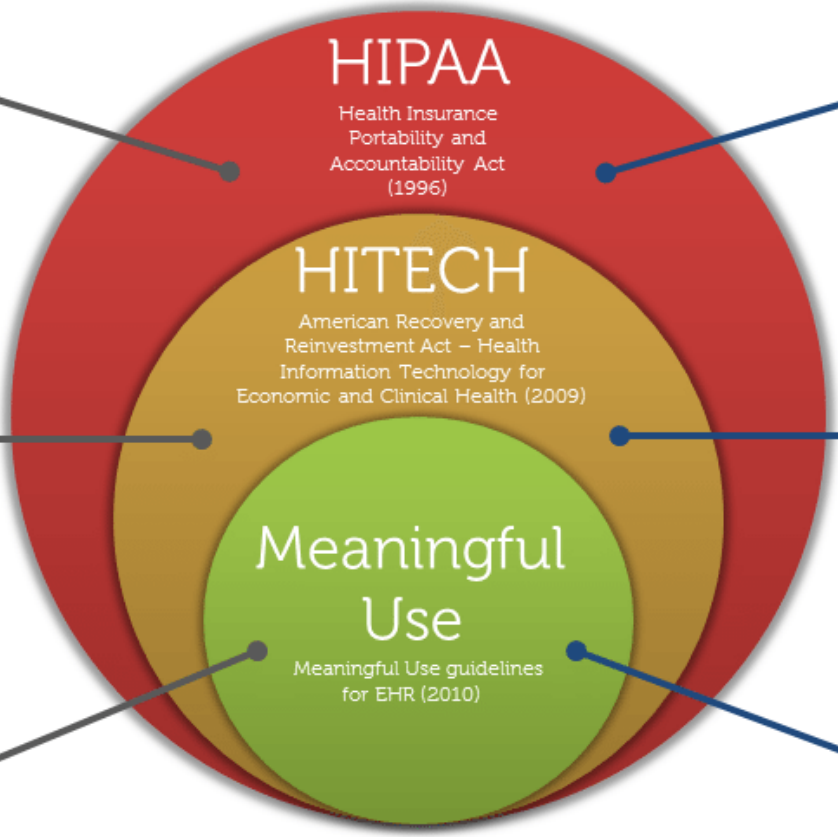
However, enforcement was very limited.

HITECH, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

It broadens the scope of privacy and security protections listed under HIPAA and also increases the repercussions and enforcement potential for non-compliance.

CMS' Meaningful Use incentive program provides incentive payouts to eligible professionals, eligible hospitals, and CAHs that meet criteria for efficient and patient-centered use of EHR.

The program provides incentives to further encourage compliance measures set forth in HITECH and HIPAA, including conducting a risk analysis.



A regulation is born:

As increasing amounts of protected health data were transferred, HIPAA was passed in 1996 to simplify the administrative processes of healthcare and to protect patients' privacy.

The Security Rule was enacted February 20, 2003, and provided administrative, physical and technical safeguards for Protected Health Information.

HIPAA gets some teeth:

HITECH extended the HIPAA Security Rule to include:

- New civil penalties for violations
- Covered entities and business associates must comply
- Breach notification obligation for breaches on or after Sept. 2009

Security gains an incentive:

Meaningful Use includes 15 core measures, including conducting a security risk analysis, updating it annually, and correcting any security deficiencies, as originally specified by HIPAA. The program offers up to $27bn over four years for attesting to all 15 objectives.

HIPAA IN A NUTSHELL

GOVERNANCE

Privacy Official

Written Policies and Procedures

Documentation About Compliance

Workforce Training

Routine Assessments

HIPAA'S SCOPE

Covered Entities (CEs)

- Healthcare Providers
- Health Plans
- Healthcare Clearinghouses

Business Associates (BAs)

people or entities that create, receive, maintain or transmit PHI on behalf of a CE

Business Associate Agreement (BAA) required to transfer PHI to BA

PROTECTED HEALTH INFORMATION (PHI)

PHI is any individually identifiable health information in any form:

oral

electronic

paper

Information is identifiable if it provides a "reasonable basis" to identify a person.

"Health information" means relating to any past, present, or future health condition or to healthcare or to payment for healthcare.

CONFIDENTIALITY AND SNOOPING

Be discrete in your communications involving PHI.

Don't leave your workstation unattended without locking access to your account.

Contain your curiosity – never snoop into people's records.

Use caution and get the patient's permission prior to discussing PHI in front of others.

MINIMUM NECESSARY RULE

Use only the minimum necessary amount of PHI for the purpose of the use.

Some exceptions:

- PHI used or disclosed to the patient
- PHI used or disclosed for treatment purposes
- PHI disclosed as required by law

SECURITY

Appropriate administrative, technical and physical safeguards to protect the privacy of PHI.

DISCLOSURES

PHI may be disclosed only with the person's authorization unless an exception applies.

Mandatory Disclosures

Some mandatory disclosures without a patient's authorization include:

- to a patient who requests PHI from his or her own records
- to HHS for a compliance investigation
- when required by law
- to report abuse

Permitted Disclosures

Some permitted disclosures without a patient's authorization include:

- to deal with a serious and imminent threat to the health or safety of the person or the public
- to respond to law enforcement requests for data
- for treatment, payment, and healthcare operations (TPO)

AUTHORIZATION

A valid authorization includes:

- who is disclosing the PHI
- who is receiving the PHI
- what PHI is being disclosed
- reason for disclosure
- how long the authorization will last
- signed and dated by the person

DATA BREACH

A data breach is an impermissible use or disclosure that compromises the security or privacy of unsecured PHI (not properly encrypted).

CE must notify HHS and affected patients "without reasonable delay" — and no later than 60 days after discovering the breach.

BAs that suffer a breach must notify the CEs that supplied them with the PHI.

PATIENT RIGHTS

Notice

receive notice of our privacy practices

Access and Copy

access their information and make a copy of it

Amendment

request an amendment to their records

Restrictions

request restrictions on certain uses and disclosures

File a Complaint

with privacy officer or HHS

Accounting for Disclosures

Patients have a right to find out about disclosures of their PHI during the past 6 years, so you must log non-TPO disclosures of PHI, whether intentional or accidental.

ENFORCEMENT

Civil enforcement by the Office for Civil Rights (OCR) at the Dep't of Health and Human Services (HHS).

Fines

Fines can be more than $1.5 million per provision violated.

Imprisonment:

Violations with a malicious motive can lead to personal fines or imprisonment.

TEACHPRIVACY

HIPAA

BASICS – HIPAA HAS 2 PARTS

PRIVACY RULE

- A set of national standards for the protection of certain health information.
- The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule — called "covered entities,"
- as well as standards for individuals' privacy rights to understand and control how their health information is used.

SECURITY RULE

- A set of regulations protecting the privacy and security of certain health information.
- The *Security Standards* (the Security Rule) establishs a national set of security standards for protecting certain health information that is held or transferred in electronic form

HIPAA

PRIVACY RULE

The Privacy Rule creates a *minimum standard* for protecting the use and disclosure of protected health information (PHI) in any medium:

paper,
electronic, or
oral information.

PHI is individually identifiable information held by a healthcare provider that concerns health status, provision of health care, or payment for health care.

Use: Sharing information *within* an organization

Disclosure: Communicating information to a party *outside* the organization

HIPAA

PRIVACY RULE STANDARDS: MINIMUM NECESSARY STANDARDS

- The Privacy Rule introduced the **Minimum Necessary Standard** to limit the amount of PHI *used*, *disclosed*, and *requested*.
- The Minimum Necessary Standard requires healthcare providers to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to, use, and disclosure of PHI.
- The Minimum Necessary Standard requires healthcare providers to limit who has access to PHI based on what they need to perform their job duties.

In other words, PHI being used and disclosed is limited to the amount reasonably necessary to achieve the intended purpose.

If you are not part of the patient care team you should not be accessing that patients chart.

HIPAA

PRIVACY RULE STANDARDS: PERMITTED USE AND DISCLOSURES

- **Use:** Sharing information *within* an organization
- **Disclosure:** Communicating information to a party *outside* the organization
- A healthcare provider may use or disclose PHI to facilitate treatment, payment, or health care operations (TPO) ***without*** a patient's written authorization:
  - **Treatment:** Provision, coordination, and management of the health care of a patient.
  - **Payment:** Activities undertaken to obtain or provide reimbursement for health care services.
  - **Operations:** Business and general administrative activities.

HIPAA

PRIVACY RULE STANDARDS: PERMITTED USE AND DISCLOSURES

- To report victims of abuse or neglect
- For workers' compensation
- For law enforcement purposes
- To avert serious health or safety threat
- In emergency situations, to notify a family member or friend

- **Remember---Must use professional judgment when it comes to sensitive situations!!!**
- **HIPAA is put in place to protect the individuals information, so use your best judgment in emergency situations.**
- **<u>Always, ALWAYS, document in the record what happens!</u>**

(Always get a form!)

HIPAA
SECURITY RULE

The Security Rule complements the Privacy Rule.

While the Privacy Rule pertains to all PHI, including paper, electronic, or oral information, the Security Rule deals specifically with electronic protected health information (ePHI).

There are three types of security safeguards required for compliance: administrative, physical, and technical.

HIPAA

SECURITY RULE STANDARDS: SAFEGUARDS

Administrative Safeguards – administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations (risk analysis & management)

Technical Safeguards – controlling access to computer systems (username and password) and protecting communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient (encryption)

Physical Safeguards – controlling *physical* access to protect against inappropriate access to PHI (locked doors, turning documents over, shredding)

Access to PHI must be restricted to only those employees who have a need for it to complete their job function.

HIM

PHI (PROTECTED HEALTH INFORMATION)

- PHI is any **INDIVIDUALLY IDENTIFIABLE** health information
  - See next slide for the **18 PHI identifiers**

Under federal law PHI is any information about health status, provision of health care, or payment for health care:

- Information doctors, nurses, and other health care providers put in your medical record
- Conversations doctors have about patient care or treatment with nurses and others
- Billing information

HIM

KNOW THE 18 PHI IDENTIFIERS

Protected Health Information (PHI) is defined as any individual identifiable information that falls into the following 18 types of identifiers:

18 Identifiers

that Constitute Individually Identifiable Health Information

1. Patient name
2. Geographical subdivisions smaller than state
3. Dates (except year) directly related to an individual, like birth, admission, discharge, and death
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/ license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web URLs
15. IP addresses
16. Biometric identifiers like finger and voice prints
17. Full-face photographic images and comparable images
18. Other uniquely identifying number, characteristic, or code

HIM

MINIMUM NECESSARY STANDARD

- When using, disclosing, or requesting PHI for purposes of **TPO** ***(treatment, payment, or operations)***, the HIPAA privacy rule requires that we limit the use and/or disclosure of PHI to the minimum reasonably necessary to accomplish the intended purpose
- The sender of PHI needs to define what falls under the category of "needs to know" instead of releasing "all" information.
- Apply this when communicating within our own organization or communicating with other organizations.

LESS IS BETTER

HIPAA

ACCESS TO PHI - THE "NEED-TO-KNOW" PRINCIPLE

The **"NEED-to-KNOW"** Principle

- PHI is shared with as few individuals as needed to ensure patient care and then only to the extent demanded by the individual's role.
- As an employee, you discuss PHI only as it applies to your job or your patient's care.

HIPAA

ACCESS TO PHI – RULES OF ACCESS

Access to computer systems and information

- Access is based on your work duties and responsibilities
- Access privileges are limited to only the minimum necessary information you need to do your work
- Access to information or an information system does not automatically mean that you are authorized to view or use all the data
- Different levels of access for personnel to PHI is intentional
- Accessing PHI for which you are not cleared or for which you have no job related purpose will subject you to sanctions

HIPAA

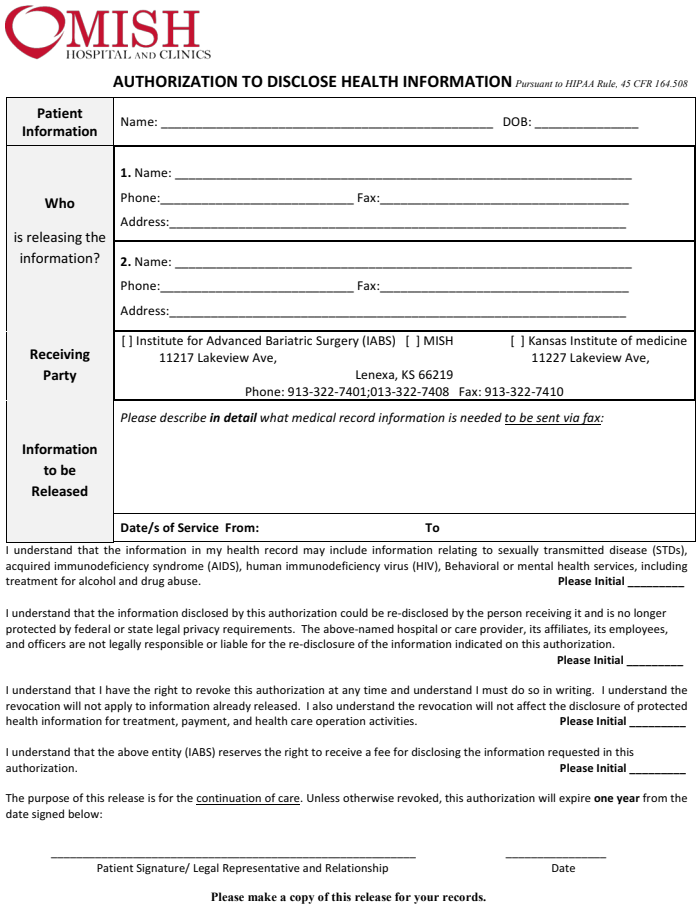
PATIENT RIGHT TO ACCESS PHI

- Ask to see and get a copy of their health records
- Have corrections added to their health information
- Receive a notice that tells them how their health information may be used and shared
- Decide if they want to give us permission before their health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why their health information was shared for certain purposes
- If they believe their rights are being denied or their health information isn't being protected, they can file a complaint with the provider or health insurer or with HHS (Health and Human Services)

HIPAA

PATIENT RIGHT TO ACCESS PHI

- Patients have a right to request a copy of their medical records
- The REQUEST must be in writing using APPROVED forms only
- ONLY designated people process PHI REQUESTS
- **30 days** are allowed for this process
- Requests can be denied under certain circumstances
- MISH employees should not access their own PHI without going through HIM Services



MISH HOSPITAL AND CLINICS

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION *Pursuant to HIPAA Rule, 45 CFR 164.508*

Patient Information	Name: _____ DOB: _____
Who is releasing the information?	**1.** Name: _____ Phone:_____ Fax:_____ Address:_____
	2. Name: _____ Phone:_____ Fax:_____ Address:_____
Receiving Party	[ ] Institute for Advanced Bariatric Surgery (IABS) 11217 Lakeview Ave, Lenexa, KS 66219 [ ] MISH 11227 Lakeview Ave, Phone: 913-322-7401;013-322-7408 Fax: 913-322-7410
Information to be Released	*Please describe **in detail** what medical record information is needed to be sent via fax:*
	Date/s of Service From: **To**

I understand that the information in my health record may include information relating to sexually transmitted disease (STDs), acquired immunodeficiency syndrome (AIDS), human immunodeficiency virus (HIV), Behavioral or mental health services, including treatment for alcohol and drug abuse. **Please Initial** _____

I understand that the information disclosed by this authorization could be re-disclosed by the person receiving it and is no longer protected by federal or state legal privacy requirements. The above-named hospital or care provider, its affiliates, its employees, and officers are not legally responsible or liable for the re-disclosure of the information indicated on this authorization. **Please Initial** _____

I understand that I have the right to revoke this authorization at any time and understand I must do so in writing. I understand the revocation will not apply to information already released. I also understand the revocation will not affect the disclosure of protected health information for treatment, payment, and health care operation activities. **Please Initial** _____

I understand that the above entity (IABS) reserves the right to receive a fee for disclosing the information requested in this authorization. **Please Initial** _____

The purpose of this release is for the continuation of care. Unless otherwise revoked, this authorization will expire **one year** from the date signed below:

_____ _____
Patient Signature/ Legal Representative and Relationship Date

Please make a copy of this release for your records.

HIPAA

PHI DISCLOSURES

- An accounting of all Patient Health Information Disclosures must be maintained
- The Disclosure LOG tracks:
  - Date
  - Place / Person disclosed to
  - Information disclosed
  - Verification of destination
  - Verification consent obtained
- Consent "Authorization to Disclose Health Information" must be obtained prior to release of the records

OMISH HOSPITAL AND CLINICS

PHI
DISCLOSURES

Patient NAME: _____ DOB: _____

ACCOUNTING OF MEDICAL RECORD DISCLOSURES

Log date/place/person patient information is being released to

Date	List Place disclosed to	List Person Disclosed to	List Information released	Was Confirmation of place / person obtained	Release authorization obtained and IN chart

HIPAA

PHI RELEASE VIA FAX

- Written Consent Obtained
- Disclosure logged
- Confirm you have the correct patients health information
- Confirm the Fax # is accurate
- Always use a Fax Cover Sheet - which includes a Tel. # for the recipient to contact us in case of a fax error.
- If a fax error occurred inform recipient to destroy the information immediately, and contact HIM Manager pr Privacy Officer.

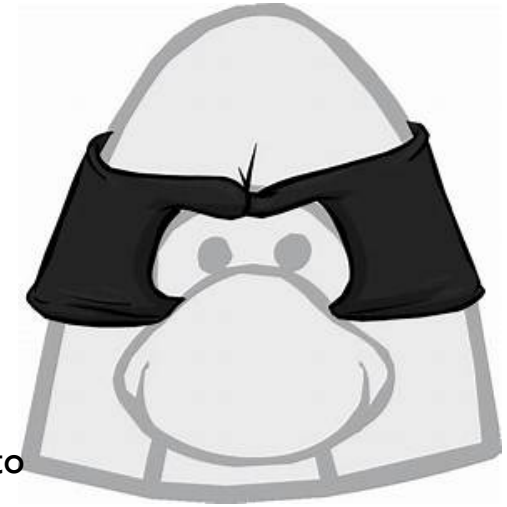
HIPAA

FEES FOR COPIES (PAPER OR DIGITAL)

- The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI
- The fee may include only the cost of:
  - labor for copying the PHI
  - supplies for creating the copy(ies)
  - postage

HIM

MEDICAL IDENTITY THEFT



- An evolving problem
- Always verify the entity requesting PHI
- Always Verify the destination the PHI is being released to
- Committed when someone uses a person's name or other parts of his/her identity to obtain medical services or goods, or falsifying claims for medical services and falsifying medical records to support those claims.
- Be aware of Red Flags: patterns, practices, or specific activities that indicate the possible existence of identity theft

If it doesn't look right, smell right, feel right …

Tell Someone!!!!!!

HIPAA

ENTITY (OUR) RIGHTS TO USE AND SHARE PATIENT PHI

HIPAA allows release of PHI:

- For patient treatment and care coordination (TPO) without consent
- To bill insurance companies for patient health care and to help run the business (TPO) without consent
- With patient family, relatives, friends, or others patient identifies who are involved with your health care or your health care bills, unless you object
- To protect the public's health, such as by reporting when the flu is in the area without consent
- To make required reports to the police, such as reporting gunshot wounds

PHI cannot be used or shared without specific patient written authorization to:

- Give patient information to the employer
- Use or share patient information for marketing or advertising purposes or sell patient information.

HIPAA

EXAMPLES OF TPO:

(PERMITTED *WITHOUT* A PATIENT'S WRITTEN AUTHORIZATION)

Treatment:

- A lab may fax, or communicate over the phone, a patient's medical test results to a physician.
- A physician may mail or fax a copy of a patient's medical record to a specialist who intends to treat the patient.
- A doctor may discuss a patient's condition over the phone with an emergency room physician who is providing the patient with emergency care.
- A doctor may orally discuss a patient's treatment regimen with a nurse who will be involved in the patient's care.
- A doctor may consult with another health care provider regarding a patient's treatment.

Payment:

- For determinations of eligibility or coverage,
- For Precertification
- For Preauthorization
- For Billing of services rendered
- For Claims Management
- For Collection activities for obtaining payment
- For Utilization Review (concurrent, retrospective)

Operations:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines
- Training staff: Reviewing competence or qualifications of healthcare professionals, evaluating performance
- Medical review, auditing, or compliance programs
- Business planning and development, cost mgmt, etc

HIPAA:

INCIDENTAL USE & DISCLOSURE

HIPAA does <u>not</u> prevent hospitals from:

- Using whiteboards on hospital floors
- Using sign-in sheets or calling patients by name at clinic desks
- Placing patient charts outside of examination\hospital rooms
- Leaving messages on patient's answering machines

HOWEVER---Precautions must be taken to safeguard the patient's privacy (limit the amount of information that might be incidentally disclosed)

<u>Examples of *reasonable safeguards*:</u>

- Keep voice low while discussing PHI or move to private location
- Turn the front of the chart towards the wall outside exam rooms so others can't see anything while passing by
- Limit the amount of information left on a patient's voicemail, request return phone call
- If a patient has visitors with them, ask if it is alright that their PHI be discussed with the visitors present

HEALTH INFORMATION MANAGEMENT (HIM)

POLICIES AND PROCEDURES

All HIM policies and procedures are available on SharePoint as *200 Information Management & Record of Care, Treatment, and Services*

All employees undergo on-hire & annual re-training to ensure compliance with:

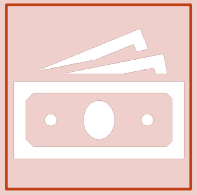
- Patient confidentiality
- HIPAA
- Patient Rights

HIM

ID BADGES - SECURITY

Employee ID badges act as an access pass throughout the building

Employee ID badges should be visibly worn by all employees while on duty



Replacement of employee ID badges will cost $20

HIPAA

MISH NOTICE OF PRIVACY PRACTICES AND PATIENT RIGHTS

- Every Patient receives a copy of **MISH Notice of Privacy Practices and Patient Rights** at time of registration
- Patient MUST sign an **acknowledgement** receipt when they receive the Notice at time of registration.
- A **copy** of MISH Notice of Privacy and Patient Rights is posted on the wall in the Main lobby at all times
- When a patient is admitted, they also read and sign **MISH Conditions of Admission** that reiterates the patient's rights regarding use and disclosure of their PHI.
- The patient is able to request an "accounting of disclosures", meaning we can tell them who has requested their records and to whom we released them to. ***(This is why it is important to track all releases of information.)***

MISH HOSPITAL AND CLINICS

PATIENT RIGHTS AND SERVICES

At The Minimally Invasive Surgery Hospital (MISH), we're committed to making your hospital experience the best possible. That means quality care, attentive staff, high quality and efficient service. Health care delivery is enhanced by the involvement of the patient and family as partners with our staff in the health care process. In the spirit of mutual trust and respect, it is our responsibility to advise you of your rights as a patient, your legal rights regarding healthcare treatment decisions, and to identify your role and responsibilities in your treatment and care. It is also our responsibility to address your concerns to assure your

ask questions, be proactive and take

have questions or concerns, we enco

Nursing or our Patient Advocate.

Questions About Your Care

complex processes. There may be

concern. If that happens, below you

and resolve your concerns in a way tha

Here's how:

Point of Contact

The best time to address any concern

your care, your service or even your f

our staff to listen carefully to our pat

that emphasizes an attentive, timely r

the person who provides your care

immediately and help avoid any recur

needs, so we have the opportunit

Call the Director of Nursing

Not comfortable talking with the pers

speak with the director of nursing.

immediately. Our goal is to answer yo

as possible to help ensure you receive

our attention to a problem will never

though we try, we know perfection isn

to make things right.

Call the Patient Advocate

Because we realize some problems

provide a special staff member – calle

a liaison between you, your family an

every department and every staff member to assure your situation is addressed and resolved. To reach the Patient Advocate call 913-322-7408. The Patient Advocate is available Monday through Friday, from 9 a.m. to 5:00 p.m. The Patient Advocate will investigate your concerns within three working days of your call and he will keep in touch with you until your situation has been resolved.

Advance Complaint and Grievance Resolution Process

Any concern that isn't resolved promptly is called a grievance. You may lodge a grievance by contacting the Patient Advocate. Your grievance will be resolved as quickly as possible, and you will receive a written response on the subject within 30 days. Exercise your right to the grievance process freely without being subject to coercion, discrimination, reprisal or unreasonable interruption of care. In addition, we

MISH HOSPITAL AND CLINICS

NOTICE OF PRIVACY PRACTICES

ADMINISTRATIVE SIMPLIFICATION PRIVACY SECURITY TRANSACTIONS

This notice describes how health information about you may be used and disclosed and how you can get access to this information. Please review it carefully. If you have any questions about this notice, please contact the Privacy Officer by dialing the main hospital number.

Our Responsibilities

We are required by law to maintain the privacy of your health information and provide you a description of our privacy practices. We will abide by the terms of this notice.

Uses and Disclosures:

How we may use and disclose Health Information about you.

The following categories describe examples of the way we use and disclose health information.

For Treatment: We may use health information about you to provide you treatment or services. We may disclose health information about you to doctors, nurses, technicians, health students, or other hospital personnel who are involved in taking care of you at the hospital. For example: a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. Different departments of the hospital also may share health information about you in order to coordinate the different thi

x-rays. We may also provic

copies of various reports t

discharged from this hospita

For Payment: We may use

services to bill and collect

about your surgery so they

tell your health plan about

your plan will cover it.

For Health Care Operations

team may use information

your case and others like it

quality of care for all patient

We may also use and disclo

- To business associ

service and billing f

- To remind you that

- To assess your satisfaction with our services;
- To tell you about health-related benefits or services;
- To contact you as part of fundraising efforts;
- To inform Funeral Directors consistent with applicable law;
- For population based activities relating to improving health or reducing healthcare costs; and
- For conducting training programs or reviewing competence of healthcare professionals.
- When disclosing information, primary appointment reminders and billing/collections efforts, we may leave messages on your answering machine or voice mail.

Business Associates: There are some services provided in our organization through contracts with business associates. Examples include physician services in the radiology department, certain laboratory tests, and a copy services we use when making copies of your health record. When these services are contracted, we may disclose your health information to our business associate so that they can perform the job we've asked them to do and bill you, your insurance company or a third-party payer for services rendered. To protect your health information, however, we require the business associate to appropriately safeguard your information.

Research: We may disclose information to researchers when an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your health information has approved their research and granted a waiver of the authorization requirement.

il outs or disease-latives or

bers have on will be erations. n in their ne. following

ontrolling

PLEASE READ THE NOTICE of PRIVACY PRACTICES and PATIENT RIGHTS and SERVICES HANDOUT PROVIDED TO YOU PRIOR TO SIGNING BELOW. IF YOU HAVE ANY QUESTIONS OR WOULD LIKE MORE INFORMATION, PLEASE CONTACT OUR DIRECTOR OF QUALITY, AT 913-322-7401.

Notice of Patient Rights and Services

At The Minimally Invasive Surgery Hospital (MISH), we're committed to making your hospital experience the best possible. That means quality care, attentive staff, high quality and efficient service.

Health care delivery is enhanced by the involvement of the patient and family as partners with our staff in the health care process. In the spirit of mutual trust and respect, it is our responsibility to advise you of your rights as a patient, your legal rights regarding healthcare treatment decisions, and to identify your role and responsibilities in your treatment and care. It is also our responsibility to address your concerns to assure your satisfaction and your good care. We urge you to read the Patient Rights and Services handout for full disclosure and ask questions, be proactive and take an active part in your health care plan. If you have questions or concerns, we encourage you to discuss these with the Director of Quality or our Patient Advocate.

Notice of Privacy Practice

Minimally Invasive Surgery Hospital (hereinafter called MISH) is required by law to maintain the privacy of certain confidential health care information, known as Protected Health Information or **PHI**, and to provide you with a notice of our legal duties and privacy practices with respect to your PHI this is provided to you in the form of the Notice of Privacy Practices Handout. This Notice summarizes MISH's legal responsibilities as well as your legal rights, advises you of our privacy practices, and lets you know how MISH is permitted to use and disclose PHI about you. MISH is also required to abide by the terms of the version of this Notice currently in effect. We may use this information as described in this Notice without your permission. We respect your privacy, and treat all health care information about our patients with care under strict policies of confidentiality that all of our staff are committed to following at all times.

***Revisions to the Notice**: MISH reserves the right to change the terms of this Notice at any time, and the changes will be effective immediately and will apply to all protected health information that we maintain. Any material changes to the Notice will be promptly posted in our facility and posted to our web site. You can get a copy of the latest version of this Notice by contacting the Privacy Officer identified above.*

MISH may be required to report certain medical information for public health purposes. For instance, we are required by law to report communicable diseases to the state and the CDC. We also may need to report patient problems with medications or medical products to the manufacturer and to the FDA, or may notify patients of recalls of products they are using.

I hereby acknowledge that I have been provided with a copy of Minimally Invasive Surgery Hospital's Notice of Privacy Practices and the Patients Rights and Services Handout.

Signature of Patient, Parent, Guardian or Personal Representative *Date*

Signature of Guardian or Personal Representative *Date*

MISH HOSPITAL AND CLINICS

Acknowledgment
Notice of Privacy
Practice - Patient Rights

HIPAA

DON'T'S


HIPAA
Don'ts
1 Don't keep patient info sheet at front desk
2 Don't access PHI on non-secure mobile phone or connections
3 Don't share your patient information on social media
4 Don't access patient records without proper/valid business reason


What can't I do?
Share that you serve a celebrity to gain more credibility for your practice*
Celebrities are protected under HIPAA and sharing that they attend your practice without consent is a violation.
Include patients in a newsletter if they have not signed a consent form*
If you mention a new newsletter campaign, and a patient verbalizes that they'd like to take part, including them is a violation unless they sign a consent form.
Post pictures of patients receiving treatment*
Nearly all photos in brochures and at office spaces are stock photos.
Share a patient's own post about their experience*
If someone outwardly shares their own health information online, it is not compliant to share their experience to your followers, just because they've decided to publicize their experience.
Provide false testimonials
Using a testimonial that is false is non-compliant.
Sell protected health information to third parties*
Hospitals cant sell names to magazines, businesses, etc. without authorization.
Share health information with a telemarketer*
Only if the covered entity has obtained a written authorization to do so or if there is a business/associate relationship present.
Statements with an *, dictate that this action can be done with a proper HIPAA authorization

HIPAA

DONT'S

SOCIAL MEDIA

Never post about patients

It's extremely difficult to anonymize patients - even the subtlest identifier could land you and your practice in a lot of trouble.

Only use secure messaging

Only discuss or exchange patient information using HIPAA-secure messaging platforms.

Educate yourself and others

Staff should always be trained and kept up to date with HIPAA compliance best practices and company social media policies.

Don't mix work and personal life

Healthcare professionals should keep their personal and professional lives separate. Interacting with a patient online could result in PHI inadvertently being exchanged in the public domain.

When in doubt, don't post

People can make mistakes in the heat of the moment. Always take a minute, read the post back to yourself, and consider the potential consequences before hitting the 'post' button

HIPAA:

DON'T'S DIGITAL DATA SECURITY

- NO thumb drives.
- NO charging cell phones from computers.
- NO connecting any device to MISH computers or network.

HIPAA:

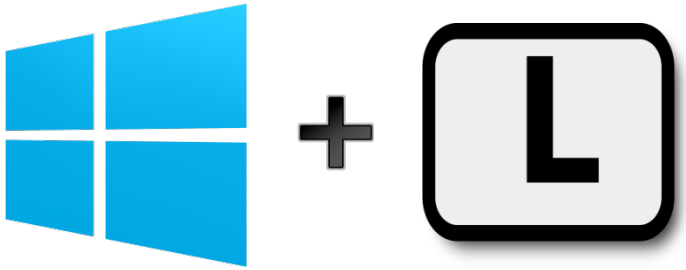
DONT'S COMPUTERS

- All data on computers must be kept OUT of patient view.
- Computers are for business use ONLY. Do not assume messages, e-mails are private.
- Abusing computer privileges will be subject to disciplinary action.
- Do not open emails with links/attachments unless you are 100% sure of the source. **REMEMBER- THINK BEFORE YOU CLICK.**
- NO creating shortcuts!
- Be sure to always save your documents to the "M"- Drive in case the computer crashes so information is not lost.

HIPAA

PROTECTING PHI ON COMPUTERS

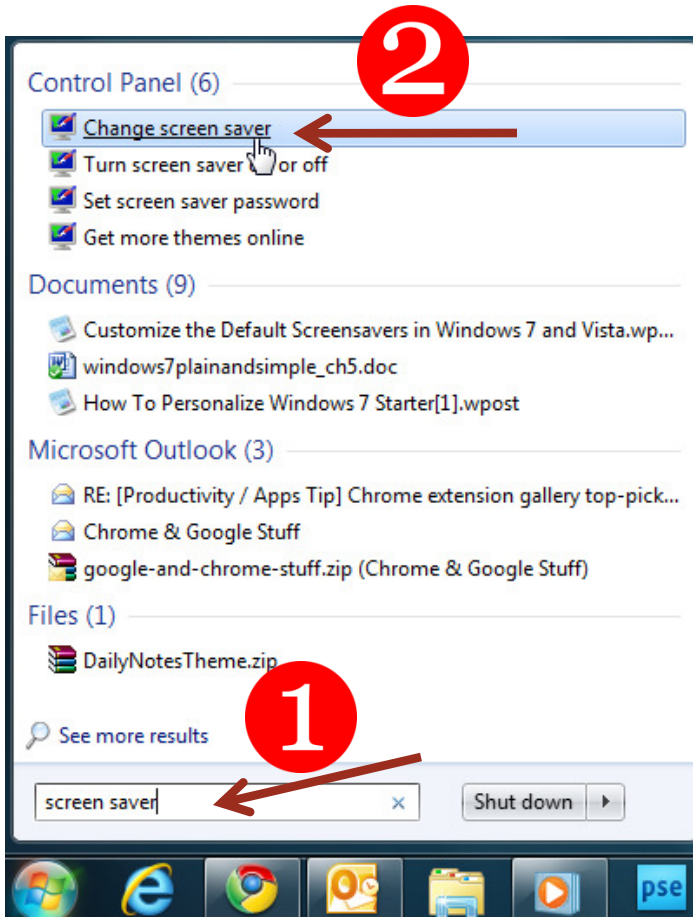
- NO sharing passwords.
- Every employee has their *own* logon and password.
- Always go to "switch user" on a shared computer (ex. nurses station)
- Always work on a computer or access information under your own account name
- Employees must **lock computers** when leaving workstations:
  - **Windows Key + "L"**
  - Start button then click Lock
  - Press Ctrl, Alt, Delete then Enter

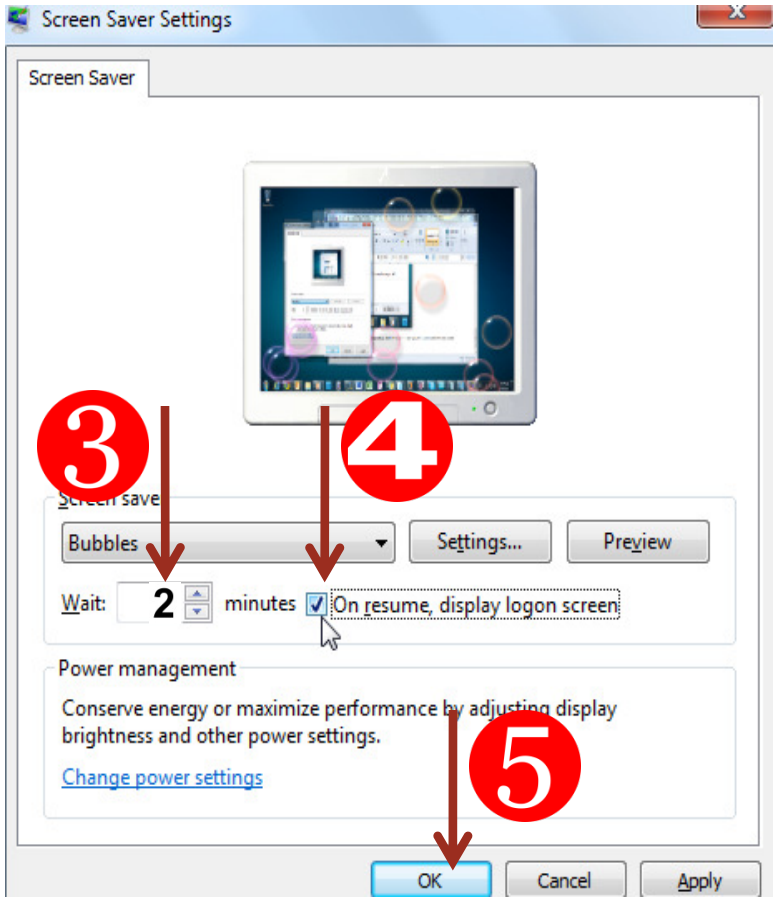


HIPAA:

PROTECTING PHI ON COMPUTERS

- Employees must enable the auto-lock feature to prompt the screensaver to come on after **2** minutes of inactivity. Upon resume, the logon screen will be display requiring a password.





HIPAA

MYTHS

DISPELLING COMMON MYTHS SURROUNDING HIPAA

MYTH 1: A patient can take the medical practitioner to court for a privacy violation.

FACT: No. Even if the medical practitioner commits the worst kind of privacy violation, the affected patient can complain to the Secretary of Health and Human Services (HHS). Appropriate investigations and penalties, if applicable, will be imposed by HHS and enforced by the Department of Justice (DOJ).

MYTH 2: Medical practitioners are allowed to share patients' personal health information with their employers.

FACT: No. Employers can only get access to a patient's personal health information if the patient is their employee, but only with the patient's written consent.

MYTH 3: The patient's family members are not allowed to pick up prescriptions and other related documents.

FACT: No. The patient's family members are authorized to receive documents such as prescriptions, X-rays and other medical records.

MYTH 4: Medical practitioners cannot share a patient's health information with his or her family without written permission.

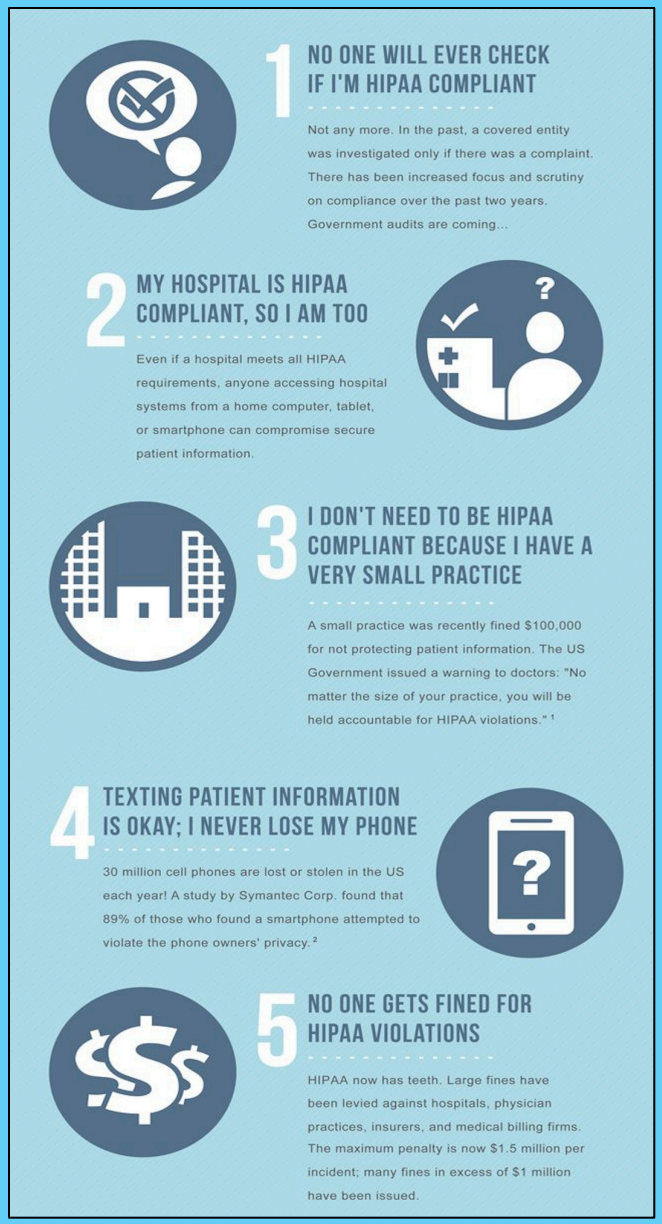
FACT: No. If the situation demands, the patient's health information can be shared with a family member or a close associate even without a formal written consent.

MYTH 5: A doctor cannot send a patient's medical records to another doctor without the patient's written consent.

FACT: No. A doctor does not require a written consent to transfer a patient's medical records to another doctor for treatment purposes.

HIPAA

MYTHS


1
NO ONE WILL EVER CHECK IF I'M HIPAA COMPLIANT
Not any more. In the past, a covered entity was investigated only if there was a complaint. There has been increased focus and scrutiny on compliance over the past two years. Government audits are coming...
2
MY HOSPITAL IS HIPAA COMPLIANT, SO I AM TOO
Even if a hospital meets all HIPAA requirements, anyone accessing hospital systems from a home computer, tablet, or smartphone can compromise secure patient information.
?
3
I DON'T NEED TO BE HIPAA COMPLIANT BECAUSE I HAVE A VERY SMALL PRACTICE
A small practice was recently fined $100,000 for not protecting patient information. The US Government issued a warning to doctors: "No matter the size of your practice, you will be held accountable for HIPAA violations." [1]
4
TEXTING PATIENT INFORMATION IS OKAY; I NEVER LOSE MY PHONE
30 million cell phones are lost or stolen in the US each year! A study by Symantec Corp. found that 89% of those who found a smartphone attempted to violate the phone owners' privacy. [2]
?
5
NO ONE GETS FINED FOR HIPAA VIOLATIONS
HIPAA now has teeth. Large fines have been levied against hospitals, physician practices, insurers, and medical billing firms. The maximum penalty is now $1.5 million per incident; many fines in excess of $1 million have been issued.

HIPAA

MYTHS

Myth #1

"I don't bill Medicare, so I don't need to follow HIPAA Rules"

All covered entities must abide by HIPAA Privacy and Security Rules. Covered entities include healthcare providers, health plans and healthcare clearing houses. Only healthcare providers who do not transmit claims electronically meet an exception.

Myth #2

"As the patient, I own my whole medical record and I want it now."

HIPAA allows individuals the Right to Access and to receive a copy of the Designated Record Set within 30 days. However, the patient does not have ownership of the entire medical record. The provider "owns" the medical record.

Myth #3

"While looking up a patient on the EHR, I accidentally looked up the wrong patient. This is a breach and it needs to be reported."

Not every impermissible use or disclosure is considered a breach. Under HIPAA, there are exceptions to what is a true breach requiring breach notification, such as in this case. Keep in mind that if the impermissible use or disclosure does not meet one of the exceptions, there are strict deadlines to meet under the Breach Notification Protocol to avoid violations and subsequent penalties for untimely reporting.

Myth #4

"Since it was my Business Associate, a billing company that caused the large breach of PHI, I am off the hook."

With a valid written Business Associate Agreement (BAA), this may be true in regard to the financial harm from penalties for a breach by the Business Associate, but this may not prevent significant reputational harm to the covered entity.

Myth #5

"In the waiting room, the nurse should not call out my name [PHI] when it's time to see the doctor."

This is an example of an Incidental Use which is permitted by HIPAA. However, there are many ways that PHI may be impermissibly disclosed from your facility. An unsuspecting employee can easily be the source of a breach of PHI by simply opening or sending an email.

HIPAA

TOP BREACH'S

HIPAA

VIOLATION EXAMPLES

HIPAA

Who does HIPAA apply ?

EVERYONE!!!

HIPAA

HOW TO HANDLE A COMPLAINT

1 Timely Respond to Patient Complaints

The clock is ticking if there is a breach of PHI. Penalties can be avoided/reduced if corrected within

30 DAYS

2 Conduct an Adequate Investigation

3 Correct and Mitigate Harmful Effects

4 Determine if there is a Reportable Breach

Do not report if an exception applies:

- Unintentional access that does not result in further use or disclosure that violates HIPAA.
- An inadvertent disclosure of PHI
- Good faith belief that the unauthorized person would not likely retain the PHI

Report the breach If there is more than a low probability of PHI compromise based on a risk assessment of the 4 factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

5 Involve HR to Determine Disciplinary Measures

HIPAA requires covered entities to sanction employees who violate HIPAA. Work with HR to identify the appropriate disciplinary measures to take.

6 Document and Record all Investigative Efforts

7 Follow up with the Patient

Notify the patient of the findings and resolution of their complaint.

Click the link below for a sample HIPAA Privacy Complaint Form.

WHAT IF I HAVE HIPAA ?'S

- Read MISH Notice of Privacy Practices
- Ask your Supervisor
- Ask Medical Records Manager
- Ask the Privacy Officer
- Re-read THIS Power Point!!
- **NEVER** hesitate to reach out for help when presented with an official document requesting PHI.
    - Ex: Law Offices, Law Enforcement, Medicare/Medicaid Audits, Social Security Administration

When in doubt– Ask the Privacy Officer!

PATIENT RIGHTS

- Every Patient has the Right to:
  - Be treated with dignity and respect
  - Have privacy and confidentiality concerning healthcare
  - Have their questions, concerns, or complaints addressed in good faith
  - Be provided with current, comprehensive information about their healthcare
  - Make decisions concerning their care
  - Be given necessary information prior to consenting to a procedure or treatment (informed consent)
  - Receive requested information about fees and charges and an explanation of their bill
  - Receive a copy of their medical record, if requested (must have release of medical records authorization signed by patient)
  - Expect reasonable continuity of care
  - Have the option of an advance directive concerning treatment or designation of a surrogate decision maker

PATIENT RIGHTS

- Every Patient has the Right to:
  - Understand and use these rights. If for any reason you do not understand or you need help, the hospital must provide assistance, including an interpreter.
  - Receive treatment without discrimination as to race, color, religion, sex, national origin, disability, sexual orientation, or source of payment.
  - Receive considerate and respectful care in a clean and safe environment free of unnecessary restraints.
  - Receive emergency care, as you need it.
  - Be informed of the name and position of the doctor who will be in charge of your care in the hospital.
  - Know the names, positions, and functions of any hospital staff involved in your care and refuse their treatment, examination or observation.
  - A no smoking room.
  - Receive complete information about your diagnosis, treatment and prognosis.
  - Receive all the information that you need to give informed consent for any proposed procedure or treatment. This information shall include the possible risks and benefits of the procedure or treatment.

PATIENT RIGHTS

- Every Patient has the Right to:
  - Refuse treatment and be told what effect this may have on your health. (In this case, an AMA form shall be filled out)
  - Refuse to take part in research. In deciding whether or not to participate, you have the right to a full explanation.
  - Privacy while in the hospital and confidentiality of all information and records regarding your care.
  - Participate in all decisions about your treatment and discharge from the hospital. The hospital must provide you with a written discharge plan and written description of how you can appeal your discharge.
  - Review your medical record without charge. Obtain a copy of your medical record for which the hospital can charge a reasonable fee. You cannot be denied a copy solely because you cannot afford to pay.
  - Receive an itemized bill and explanation of all charges.
  - Complain without fear of reprisals about the care and services you are receiving and to have the hospital respond to you; and if you request it, a written response.