TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER
HEALTH.EDU

CHECKpoint III: Patient Protections
(PROGRAM: 40623)

Presenter: Narrated

COURSE OBJECTIVES

- Discuss patient rights, privacy standards, informed consent, advance directives, and laws regarding protected health information such as HIPAA and HITECH.
- Identify computer security and good practices, as well as the responsible use of social media.
- Recognize types of and prevention methods for adverse medical events and errors, and the potential for problems related to alarm fatigue.
- Identify mandatory reportable incidents of abuse and how to recognize abuse in healthcare settings.

Module 1: Patient Rights and Maintaining Patient Privacy

Patient's Bill of Rights

Patients have rights in healthcare facilities that are guaranteed by law. The Patient's Bill of Rights under the Affordable Care Act (ACA) allows people with pre-existing conditions access to health insurance coverage, provides certain preventative screening without paying an extra fee or co-pay, and stops health plans from canceling policies when patients become sick. People have a right to choose their primary care doctors and to appeal if denied coverage.

Patients have the right to pain management, reasonable accommodation for religious or other spiritual services or practices, and the right to choose who may visit them in the hospital. Institutions MAY NOT deny visitation privileges on the basis of race, color, national origin, religion, gender, sexual orientation, gender identity, or disability. They must have and enforce policies against that discrimination and educate all patients about their rights.

While in a healthcare facility, patients have the right to considerate, respectful care and may not be discriminated against in the delivery of services based on race, ethnicity, national origin, religion, culture, language, physical or mental disability, socioeconomic status, sex, sexual orientation, gender identity or expression, age, genetic information, or source of payment.

Patients should be informed about the internal complaint and grievance resolution process, and be informed of available resources to resolve conflicts, grievances, or disputes when they are admitted. Patients have the right to voice complaints freely and recommend change

without being subject to coercion, discrimination, reprisal, or unreasonable interruption of care, treatment, and services.

Patients have the right to seek out emergency care, even out of their healthcare provider network.

Patients who think that they may be experiencing an emergency medical condition have the right to go to an emergency department, request examination or treatment, and be provided an appropriate medical screening examination to determine if such a condition exists. Patients have the right to this examination, and to receive treatment until stable, regardless of their ability to pay. This is further discussed in the section on EMTALA.

Patients have a right to make treatment and care decisions, and to take part in decisions about their care. Those who cannot make their own decisions may identify someone to help make decisions for them. Patients have the right to accurate, easy-to-understand healthcare information in their primary language. Patients who don't speak English, or have disabilities that make it difficult to understand, must be provided translation and communication services so they can make informed healthcare decisions.

Patients have the right to have information about their decisions and treatments kept confidential. Patients have the right to privacy when talking about healthcare information to healthcare providers. They have the right to read their medical record and to ask that it be changed if it is not accurate. Patients have the right to have information explained or interpreted, as necessary, except as restricted by law.

Patients have the right to consent to, withdraw from, or decline to participate in research studies or human experimentation that affects care and treatment or requires direct patient involvement, and to have those studies fully explained before consent. Some states and health facilities have enacted additional laws and policies that provide additional patient rights. Know the laws in your state and your facility policies.

EMTALA

The Emergency Medical Treatment and Active Labor Act (EMTALA) gives patients the right to receive emergency medical treatment at a hospital regardless of the ability to pay or medical insurance. EMTALA laws do not apply to outpatient facilities, unless it is an urgent care facility owned by a hospital that bills under the hospital's provider number as an outpatient department of the hospital. EMTALA requires that every patient seeking emergency care, including women in active labor, receives the following:

- A medical screening exam, which includes tests, consults, or whatever is needed to determine whether or not the patient has an emergency medical condition (EMC)
- Stabilizing treatment within the hospital's capability and room for the patient
- Admission for further treatment if the hospital has the capability and room to treat the patient, or transfer the patient if the hospital does not have the capability or the room to treat
- Or lastly, treatment and discharge of the patient

Hospitals are not allowed to get pre-authorizations for treatment or to confirm a patient's insurance until after the medical screening exam, stabilizing treatment, and determination if an emergency medical condition exists. Hospitals also must perform "lobby rounding" when patients are not being placed into a patient bed immediately after being triaged, but are seated in the waiting area until a bed becomes available. Lobby rounding monitors these patients to ensure their condition doesn't deteriorate.

A hospital is responsible for all areas 250 yards around the main building and around areas where inpatient services are provided. This area includes parking lots, sidewalks, and access ways, but not public streets or other private businesses.

Under most conditions, a patient is considered to have arrived at the hospital and EMTALA rules start on entering a hospital-owned ambulance.

Facilities are not violating EMTALA rules if a patient leaves against medical advice or leaves without being seen unless it can be proven healthcare staff encouraged a patient to leave. This would include if staff told a patient it would be hours before he or she was going to be seen, said it's going to be less expensive to go to the urgent care center, or said the hospital wasn't a provider for the patient's insurance company. If any of those things are said to the patient, the enforcement agency for EMTALA, CMS, has a tendency to side with the patient. Hospitals should document conversations with patients, especially when they leave against medical advice, and try to get release forms signed by the patient before they go that include a doctor's signature, and information that the doctor spoke with the patient.

Hospitals with specialized skills must accept transfer patients from other hospitals that lack the means to care for those patients. If a patient is unstable, a hospital cannot transfer the patient.

There are times hospitals may declare diversionary status under CMS guidelines, but they are still obligated to provide care for a patient brought to their doors during this time.

During a disaster or pandemic disease outbreak, CMS may allow waivers for hospitals for certain EMTALA obligations.

EMTALA gives patients the right to sue hospitals and physicians, and CMS could also fine hospitals from $25,000 and $50,000.

Informed Consent

Patients have the right to participate in treatment options and make decisions about their care. Patients decide on treatment through a process called informed consent. Informed consent is a process, not just a form. Informed consent is the communication between a patient and physician that results in the patient's authorization or agreement to undergo a specific medical intervention. Physicians have an ethical and legal duty to provide patients the information necessary to be fully informed before deciding to undergo major treatment. This informed consent must be documented in writing.

An informed consent may be withdrawn at any time and more information may be requested at any time. Electronic consent can now replace written consent as the legal documentation of consent.

All medical care requires the consent of a patient or a person authorized to consent for the patient. Authorization could be agreeing with a doctor's plan and filling a prescription. This is called implied consent. More detailed medical care, like most surgeries, cancer treatments, vaccines, and some blood tests, require signed documentation BEFORE treatment. This is called written informed consent.

Every state has laws regarding informed consent, but they may vary. Failure to obtain informed consent makes any physician practicing under a United States medical license liable for negligence or battery. These behaviors represent medical malpractice. Exceptions exist for medical emergencies or when mental incompetency or physical incapacity has been legally determined.

Patients should be notified and have common items explained during the informed consent process by a doctor – not a representative. The American Medical Association recommendations for informed consent include:

- The health problem, necessity of treatment or if it can be postponed, and the purpose of treatment
- What occurs during the treatment or procedure
- Risks and benefits of the treatment or procedure

- Risks and benefits of alternative treatments or procedures, regardless of cost or whether they are covered by insurance
- Risks and benefits of not receiving any treatment or procedure

A properly completed informed consent form, which meets the minimum federal requirements, must be in the patient's health record prior to surgery. Your institutional policies may allow or require the use of standardized or generic informed consent forms. Electronic signatures are considered an acceptable alternative to a written signature. These forms must be used along with significant patient education and communication. Physicians should document the details in a patient's medical record.

Some of the best practice recommendations for obtaining informed consent include, but are not limited to, the following:

- Provide patients with information fact sheets to take home to review and discuss with family and caregivers
- Use other educational tools including videos, images, animation, and computer-based training
- Ask patients to repeat information back in their own words to ensure proper understanding
- Invite the patient to ask questions and respond respectfully
- Always make sure patients are made aware of their rights to decline procedures
- Assess for and respect patient preferences related to personal, religious, and other cultural values and beliefs
- Use language both in person and on printed materials, that's simple and easy to understand
- Use a consistent outline or template for consent forms

Information must be given to the patient in a language or way that the patient understands. Patients who don't speak English or have disabilities that make it difficult to understand must be provided help, such as translators or interpreters, so they can make informed healthcare decisions. Institutions that receive federal funding are required to use interpretation and translation services for individuals with limited English proficiency, if the language is spoken by five percent or 1,000 of a provider's patients, whichever is less.

The informed consent form should include:

- Name and signature of the patient, or if appropriate, legal representative
- Name of the institution
- Name of the procedure

- Name of all practitioners performing the procedure and the significant individual tasks if more than one practitioner is involved
- Risks
- Benefits
- Alternative procedures and treatments and their risks
- Date and time consent is obtained
- Statement that the procedure was explained
- Signature of the person witnessing the consent
- Name and signature of the person who explained the procedure

Advance Directives

Advance directives are written instructions, recognized under the law, relating to the provision of healthcare when or if an individual is incapacitated. A patient may change or revoke an advance directive at any time.

A living will and a durable power of attorney are the two most common types of advance directives.

A living will is a written statement that instructs medical providers about the patient's wishes with regard to medical treatment at the end of life and in situations of terminal illness or permanent unconsciousness.

A durable power of attorney for healthcare or medical durable power of attorney names someone else, called a proxy, advocate, or surrogate, to make medical care decisions for the patient when and if he or she is incapable and is activated when the patient is unable to make decisions. These must be honored by law.

The Patient Self-Determination Act requires most healthcare organizations to give patients, on admittance, written notice of their decision-making rights, and policies regarding advance directives in their state and the institution where they've been admitted. Patients must be told they have the right to facilitate their own healthcare decisions, the right to accept or refuse medical treatment, and the right to make an advance healthcare directive. Healthcare workers should ask patients if they have an advance directive and they should document that fact in their medical records. Healthcare staff should be trained on advance directives. And, patients should be admitted and treated without discrimination based on whether or not they have an advance directive. A facility cannot refuse to treat a patient who does not have one.

Each state is responsible for determining laws related to advance directives. Most states require two witnesses when signing an advance directive who cannot be a relative, heir, or a

provider of the patient's healthcare. The use of specific forms is another requirement that varies by state.

By law, emergency responders must exercise all life-support measures possible UNLESS a legally valid, state-recognized "Do Not Resuscitate" (DNR) order is presented to them. Not all states have DNR statutes and most only address specific situations of cardiac or respiratory death.

You are encouraged to initiate dialogue about advance care planning in a patient-centered manner and include members of the patient's family. Include the patient's cultural values such as religious, spiritual, and moral beliefs, and other personal preferences in the discussion. Supply patients with unbiased information, including benefits and alternatives to types of care and treatment often needed at the end of life. Assess their understanding of options, and under what types of situations advance directives are to be activated, so you can clarify misunderstandings.

Patient Information Privacy: Protected Health Information, HIPAA, and HITECH

Protected Health Information (PHI)

PHI stands for protected health information. PHI is federally protected under HIPAA, the Health Insurance Portability and Accountability Act. It can be paper, electronic, or oral, and includes genetic information or specimens associated with a patient. This protected information includes a name, birth date, diagnosis, social security number, or anything else that can be used to identify a patient.

PHI includes, but is not limited to, information related to a person's past, present, or future physical or mental health condition; the management of healthcare to a person; and the past, present, or future payment for administering healthcare to a person. This information is protected under the HIPAA Privacy Rule.

HIPAA and HITECH

HIPAA applies to entities such as health insurance companies, healthcare billing companies, and healthcare providers including doctors, hospitals, labs, and pharmacies. All healthcare workers, facilities, and those overseeing healthcare are required by HIPAA to protect PHI that they have access to.

HIPAA rules are made up of the Privacy Rule, the Security Rule, the Enforcement Rule, and the Final Omnibus Rule.

The Privacy Rule puts protections and limits on who is allowed to look at and receive PHI. The Privacy Rule requires a covered entity to make reasonable efforts to use, disclose, and request ONLY the minimum amount of PHI needed. Each covered entity must provide a notice of its privacy practices. Individuals have the right to review and obtain a copy of their PHI from a company's designated records except in certain circumstances.

The Privacy Rule gives people the right to have their PHI records fixed when information is inaccurate or incomplete. A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures. A company may not retaliate against a person for assisting in a HIPAA investigation by any authority and, in most cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children.

The second component of HIPAA is the Security Rule. It establishes national standards to protect and secure PHI which is created, received, maintained, or transmitted in an *electronic form*.

The provisions in the Security Rule require companies to apply several policies and procedures for electronic PHI including:

- Risk analysis as part of their security management processes
- Authorizing PHI access based on the user or recipient's role
- Appropriate authorization and supervision of workplace members who work with electronic PHI
- Periodic assessment of security policies and procedures
- Ensuring that electronic PHI isn't improperly altered or destroyed
- Guarding against unauthorized access to electronic PHI being transmitted over an electronic network
- Taking reasonable steps to cure a breach or violation. Violations include the failure to implement safeguards that reasonably and appropriately protect electronic PHI

The Final Omnibus Rule increased HIPAA privacy and security protections. The updates also strengthened the HITECH Breach Notification requirements. The rule clarifies when breaches of unsecured health information must be reported to Health and Human Services. Covered entities and businesses must provide notification following a breach of protected health information.

Some other rights and regulations include:

- Prohibiting selling a person's PHI without their permission
- Limiting use and disclosure of PHI for marketing and fundraising purposes
- Allowing patients to instruct their providers NOT to share information about their treatment with their health plan when they pay cash
- Clarifying that genetic information is protected, and prohibiting most health plans from using or disclosing genetic information for underwriting purposes
- Allowing patients to ask for a copy of their electronic medical record in an electronic form

HIPAA does allow for the release of some PHI for patient care and other important purposes while still providing federal protections. In most cases, a covered company may NOT use or disclose PHI, UNLESS the Privacy Rule permits or requires *or* a person that is the subject of the information gives signed authorization.

Here are some examples of instances when PHI may be disclosed WITHOUT signed authorization:

- When disclosure is to the subject of the information
- When necessary for treatment, payment, and healthcare operations. Only the "minimum necessary" PHI should be disclosed and the organization to which disclosure is made must be a covered entity that has adopted reasonable safeguards
- When a person is incapacitated (for example, in an emergency situation) or not available. Informal permission may be given by asking the person to agree or object to treatment
- When needed to protect public interests, such as instances that involve abuse, neglect or domestic violence; serious health and safety threats; organ donations; research; and workers' compensation

HIPAA does NOT cut off communication between the physician and the patient's family and friends. As long as patients have given their permission, healthcare workers covered by HIPAA may provide information to anyone identified by a patient as involved in their care. Basic information such as the patient's phone and room number may also appear in a hospital directory as long as the patient has given permission.

Covered entities and businesses may use email, the telephone, or fax machines to communicate with patients and other healthcare professionals using appropriate safeguards to

protect patient privacy. HIPAA rules extend to business associates, like billing processors that perform certain functions or activities for a covered entity.

It is important to follow your facility- or business-specific policies on PHI. Treat all PHI as confidential. NEVER access PHI if you are not authorized. NEVER discuss PHI with anyone who is NOT authorized. ALWAYS make sure PHI is secure.

Failure to comply with the HIPAA Privacy Rule can result in substantial civil and criminal penalties.

Module 2: Information Technology

Computer Security

Computers, smart phones, tablets – these and other devices have become essential to many people, but they are a point of vulnerability for individuals and institutions.

Protecting your information starts with a strong password. The longer and more random a password is, the more secure it is. Try to make it 12 to 14 characters long. A password should be used on your desktop and on all portable devices.

Make your password random – use letters, numbers and symbols; a mix of numbers, symbols, and upper and lower case letters is hardest to break.

You should change your password often – ideally every 30 days and you should NOT share your password with anyone. If you think that your password has been compromised, notify the IT department and your supervisor, and change it immediately.

Do not use one password for everything – use a lengthy, strong, different password for every account. If you use the same username, email, and password for Facebook or LinkedIn that you use for your bank, and a hacker steals and decodes all the passwords for that social media site – they just got access to all your money.

How can anyone remember that many passwords? You could consider using a password manager — software that creates strong passwords every time you need one, and keeps track of them — for your personal accounts. Some institutions don't allow you to use password managers on work accounts, so check with your IT department before using one with your work account. Or use a trick that you can remember to create a random string of characters. You could use the first letters of the words in a quote, for example: "Four score and 7 years ago our fathers brought forth on this continent" could be this: Fs&7Yaofbfotc.

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER
HEALTH.EDU

One way thieves get your information is by tricking you into going to a fake site. You might see a link claiming to be to a reputable credit card site advertising a great new program. If you hover over the link you can see the URL – if it says something like this, https://www.creditcard.com/newprogram it may or may not be safe – it is safer to enter the company's address yourself.

On the other hand, you might look at the URL and see something like this: http://www.creditcard.com/newprogram=en&gws_rd=ssl#hl=en&q=https&safe=active**.lt** Notice the very end of the URL address, where it has "**dot"** in it. The letters after the LAST period in the URL indicate where it is going, so this example web address isn't going to "someplace.com," it is going to "someplace.It." Another thing to look at — the URL starts "http." The "s" in "https" stands for *secure*. These sites use a protocol for secure communication. A bank or large company would almost certainly have a URL that started http**s.** If you want to visit a site, try to avoid the links and enter the address yourself.

Follow all of these steps for safe computing, on both your work devices and your personal devices:

* Use a password or other user authentication. Use two-factor authentication if available
* Never tell anyone your password, and don't write it down and leave it near your computer
* Install and enable encryption
* Disable and do not install or use file sharing applications. Never go to illegal file sharing sites like BitShare – they are full of malware
* Install and enable a firewall
* Install and enable security software, and keep it up-to-date
* Use the latest operating system, and install updates and patches
* Research mobile apps before downloading. Malware can be in apps – use an antivirus app on your smart phone or device
* Use encryption and adequate security to send or receive health information over public Wi-Fi networks
* Delete all stored health information before discarding or reusing the mobile device
* Don't visit or download from unfamiliar websites, and do install a reliable surfing tool to evaluate the safety of places on the web
* Delete spam emails unread
* Turn your preview pane off for email, and don't open email if you don't know the sender

- Malware can be in documents such as PDFs so update your PDF reader frequently, and don't trust attachments that you are not expecting
- Avoid pop-up windows at websites; they are a common way to get infected
- Don't fall for scareware — scareware is a fake message that warns you that your computer is infected with a virus; this is a common way to trick you into downloading malware

Be alert to the physical security of your computer. Your computer is like a door into your company's network — leaving it unsecured is the same as leaving the door open to everything on that network — all the computers as well as all the information they hold.

Be aware of the actual space around you. Do NOT enter a password if someone is watching.

- Log off when you leave your station or device. Do not allow coworkers to use your work station without logging on as a new user
- NEVER leave your computer, laptop, or other device unattended
- Ask for identification if someone tells you they need to add programs to your computer or device. Your IT staff will have their ID with them.
- Be careful of downloading programs to your work device. Ensure that your facility approves of the program, application, etc.
- Keep track of CDs and DVDs, flash drives, or external hard drives

If you start having trouble with your computer — your password doesn't work, the computer is running slower, you suspect someone tried to use your computer — report the incident to your supervisor. Also, make sure IT knows what happened in detail and when it occurred. Be sure to follow your employer's specific policies, and ask your supervisor or privacy officer if you aren't sure what to do.

Electronic health records make safe computing even more essential. Patients' lives can be on the line, and procedures surrounding down times are critical.

If computers or devices go down during a planned or unplanned event, follow your institution's or department's downtime policy regarding patient care and operations. Planned downtime may include scheduled maintenance and system updates or upgrades. Unplanned events would be system failures or power outages.

Accrediting agencies require facilities to have a written plan for managing interruptions to information processes, either paper-based, electronic, or a mix of the two, and to train staff on appropriate downtime procedures. Know what is expected of you during a downtime to help reduce errors in documentation. Your facility will have a backup of electronic information

systems and will have health IT downtime and reactivation policies. It will also have downtime drills that involve frontline staff end-users. Follow your facility's policies and guidelines.

A good resource about safe computing and health IT is the government website https://healthit.gov/safer/. They also have practical tips on protecting health information and the safe use of mobile devices such as tablets and smartphones.

Responsible Use of Social Media

Using social media responsibly is critical. Social media can be used in many beneficial ways in healthcare including:

* Professional connections
* Speedy communication with staff, patients, and families
* Marketing and communication about events
* And information for patients about healthcare workers and systems

But an employee using social media can knowingly or unknowingly reveal too much information and violate patient privacy and confidentiality. Most cases are just mistakes. One common mistake is posting comments about patients that describe them with just enough detail to be identified — like a nickname, diagnosis, or room number. Another mistake is thinking social media information or a post is private and only available for the intended recipient, which is not true. Once information is released, it is always available, either on a server, screenshot, or somewhere else on the Internet. There have been lawsuits when healthcare workers referred to patients in a degrading or demeaning way or posted photos or videos of patients without consent.

Use of social media technologies must follow the current laws and standards that govern information and information technology.

Be sure to consider the threats and understand how to stop potential risks before using social media.

Follow your company's policies, guidelines, or position statements on social media. Policies vary from being extremely restrictive to open, but typically, the social media guidelines will let you know the following:

* Who can use the company's network to access social media on an employee computer or personal device
* Types of social media sites allowed to be viewed from the company's network
* Inappropriate uses of social media and punishments for violating the policy

Social media policies usually apply to employees while at work, or away from work conducting professional business, but not to non-healthcare related use off the clock. You must still understand patient privacy and confidentiality, and how your actions on social media, at work or away from work, can put you at risk for civil and criminal penalties. The timing of a social media post by a nurse working in a post-operative recovery area was linked to the timing a patient deteriorated to the point of death. Although the post had nothing to do with the organization or patient, social media documented distraction away from monitoring her patient's recovery from anesthesia.

Violations of HIPAA law, unethical conduct, or revealing a privileged communication in social media can include disciplinary actions, fines, or possible jail time. If the conduct violates the policies of your employer, you may face employment consequences including termination. Your organization could also face damages to its reputation, a lawsuit, or regulatory consequences.

NEVER reveal information about patients or companies via social media. Recognize the ethical and legal obligation to maintain patient privacy and confidentiality at all times.

Don't take or send patient-related images or videos on personal devices like cell phones. Don't share posts, blogs, or send information or images about a patient, or information gained in the patient relationship, with anyone unless there is a patient care-related need to disclose the information, or other legal obligation to do so.

Don't identify the patient by name or post or publish information that can lead to the identification of a patient. Don't refer to a patient in a negative way even if the patient is not identified. Do not discuss patients, employers, or co-workers in a negative way even if that person is not identified.

Don't post content or speak on behalf of an employer unless authorized to do so, and report any identified breach of confidentiality or privacy immediately.

Module 3: Patient Safety: Adverse Medical Events

Kinds and Causes of Adverse Medical Events and Medical Errors

Kinds

The Office of Inspector General of the Department of Health & Human Services describes three types of patient harm events.

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER
HEALTH.EDU

An **adverse event** is an event, preventable or non-preventable, that caused harm to a patient as a result of medical care. This includes hospital-acquired conditions, events that required life-sustaining intervention, and events that caused prolonged hospital stays, permanent harm, or death.

A **never event** – sometimes called a serious reportable event – such as surgery on the wrong patient, is a preventable error on the National Quality Forum list of specific events that "should never occur in a healthcare setting." Medicare does not pay for additional costs associated with many preventable errors, including those considered Never Events.

A **temporary harm event** is an event that requires intervention but does not cause lasting harm, such as an allergic reaction or hypoglycemia.

Using a random sample of Medicare beneficiaries discharged from hospitals over one month, the OIG found that 27% experienced care-related harm; 13.5% experienced adverse events which, in 1.5%, contributed to their deaths; 13.5% experienced temporary harm as a result of medical care.

Physician reviewers determined that 44% of adverse and temporary harm events were preventable.

To participate in the Medicare program, facilities must develop and maintain a Quality Assessment and Performance Improvement program. Facilities must "track medical errors and adverse patient events, analyze their causes, and implement preventative actions and mechanisms that include feedback and learning throughout the hospital." To standardize hospital event reporting, the Agency for Healthcare Research and Quality (AHRQ) developed a set of event definitions and incident reporting tools known as the Common Formats.

The Joint Commission recognizes three other types of events that are cause for concern – **no harm**, **close call**, and **hazardous (or unsafe) conditions**. A no-harm event is an error that reaches the patient but did not cause harm. A close call is an error that was caught BEFORE it reached a patient. A hazardous condition is one that increases the likelihood of adverse events.

The Joint Commission defines a **Sentinel Event** as "an unexpected occurrence involving death or serious physiological or psychological injury, or the risk thereof" and recommends that facilities report Sentinel Events and mandates performance of a root cause analysis after a Sentinel Event. A patient's suicide while in a staffed, round-the-clock care setting is a frequently reported Sentinel Event.

Errors are grouped into categories: surgical, product or device, patient protection, care management, environmental, radiological, and criminal.

An example of an environmental adverse event would be when a line to deliver gas to a patient contains no gas, the wrong gas, or is contaminated by toxic substances.

A patient elopement which resulted in disability or death, or an infant discharged to the wrong person, would be a patient protection error.

Examples of adverse events resulting from patient care would be a pressure injury in a bedridden patient or a patient on a restricted diet getting the wrong meal.

Medication errors are a common healthcare error. The three most frequently reported types of medication errors are:

* Omission errors or failure to administer an ordered medication dose
* Improper dose or quantity errors or any medication dose, strength, or quantity that differs from the prescribed
* Unauthorized drug errors or medication dispensed or administered that was not authorized by the prescriber. This category includes dispensing or administering the wrong drug

Surgical errors such as wrong site, wrong procedure, or wrong person errors are the least common type of medical error. The most common type of surgical error is unintended retention of a foreign object in a patient after a procedure or surgery.

Causes

Errors are usually complex and are rarely the result of one person's actions. They are often caused by communication problems and a failure when transmitting critical information between the patient and the provider, from one facility or department to another, between workers of different shifts, or between different providers.

Not following policies and guidelines often leads to errors. For example, failure to follow hand hygiene policies is known to lead to healthcare-acquired infections. Other human factors are poor labeling or poor documentation of samples, impaired workers, and poor handwriting.

Failure to educate and inadequate communication with patients can cause errors. For example, a patient who is not assessed as unable to read and therefore cannot read the directions for taking his prescribed medications or home treatment.

Patients also contribute to medical errors when they fail to comply with the treatment plan or medications, fail to admit to taking illicit drugs, fail to admit to certain lifestyles or social habits, or fail to completely disclose all medication they are taking.

Improper patient identification, incomplete patient assessment, failure to obtain consent, and inadequate patient education are all causes of medical errors.

Complex systems, such as medication systems, that rely on the involvement of several people can increase the risk of medical errors every time a document or medication changes hands.

Another potential contributor to error is multiple alarms. The Joint Commission created National Patient Safety Goal 06.01.01 to reduce the harm and improve the safety associated with clinical alarm systems in hospitals.

Patient falls are among the most common occurrences reported in hospitals and a leading cause of death in people ages 65 or older. Failure to properly assess the risk of a patient falling is a cause of adverse events. Fall risk may increase due to altered mental status, recent environmental changes, and loss of strength and balance.

Organizational contributors to medical errors include poor orientation and training. Errors often happen when healthcare workers must care for too many patients or when processes are hard to use or require repeated steps.

Poorly designed laboratory procedures, like cross-matching multiple blood samples at the same time, have contributed to errors. Equipment and devices such as infusion pumps or monitors can fail, leading to significant patient harm. Inadequate instruction and poorly designed equipment may lead to injuries.

Alarm Safety/Fatigue

When clinical alarms are heard and acknowledged, they are essential in providing care to patients in all healthcare settings. However, too many alerts and alarms create risks to patient safety because of alarm fatigue. Alarm fatigue happens when healthcare workers are exposed to a high volume of alarm noise in patient care areas and become desensitized, overwhelmed, or immune to the sound of alarms. This numbness can cause staff to miss or ignore alarm signals, or a healthcare worker might inappropriately turn down the alarm volume, turn the alarm off, shut doors, physically distance themselves from sources of noise, dismiss written “pop up” warnings, or adjust settings, with serious or fatal consequences.

False and non-actionable alarms sound when they are not set for individual patients, so they continuously go off. Some alarm sensors continuously ring because of poor skin prep and electrode placement on a patient, leading to electrodes falling off, or, because preventative maintenance was not completed, for example, checking the batteries. Sometimes, alarm default settings are not at an actionable level causing alarms to sound unnecessarily.

The ECRI (Emergency Care Research Institute) specifically lists improperly customized and improperly set alarms as two of the top ten technological hazards of 2019. The Joint Commission National Patient Safety Goal 06.01.01 is dedicated to reducing the harm and improving the safety associated with clinical alarm systems.

One way to reduce the frequency of nuisance alarms is to make alarms more actionable. "Actionable alarms" means alarms alert healthcare workers when a patient actually needs help or assistance. This would include setting clinical alarms for each patient. The most critical alarm signals should be reviewed and ways identified on how to reduce noise from these machines.

Another way to reduce the noise is to provide preventative maintenance, including proper skin prep and electrode placement, routine battery replacement, and routine electrode changes.

Staff should also be educated about how alarms work, and who is responsible to each alarms -- setting alarms, changing alarms, and monitoring them. Healthcare workers should know their facility's policy on who is allowed to set and change alarm parameters.

Finally, hospitals could create clinical alarm systems including using pagers, remote displays, enunciators, and phones to send alarm signals to designated staff. By applying these measures, healthcare facilities can help eliminate alarm fatigue and focus more on patient safety.

Strategies for Reducing and Reporting Adverse Medical Events and Medical Errors Prevention

Several strategies are known to reduce medical errors and adverse medical events.

Improve the safety of medication use by proper labeling, recording accurate patient medication information, and standardized practices.

Eliminate distractions and interruptions when checking transcribed or computerized orders or when preparing medications before administration. What the patient was, is, and will be taking should be communicated and documented accurately.

Use at least two patient identifiers at every patient interaction. Acceptable identifiers are an assigned identification number, a telephone number, birth date, or other person-specific identifier. A patient's room number is NOT an acceptable identifier. This also applies to written orders and using computerized prescriber order entry (CPOE) systems. The Joint Commission found that incorrect or miscommunicated information entered into health IT systems may result in adverse events and that interfaces built into the technology can contribute to the events.

“Wrong patient orders" can be an unintended consequence of using some CPOE systems that do not provide adequate safeguards, including at least two identifiers to assure correct patient identification before accepting orders

To eliminate healthcare-associated infections, use infection prevention and infection control strategies. These should be based on your facility’s risk assessments. Support a culture of hand hygiene awareness. Effective handwashing reduces the incidence of healthcare-associated infections. Use alcohol-based hand sanitizer, do not use artificial nails, keep nails short, and change gloves between patients. Keep hair pulled up and back.

If *C. difficile* is suspected, ONLY washing with soap and water prevents cross contamination and spread of infection.

Use evidence-based practices to prevent indwelling catheter-associated urinary tract infections, hospital-acquired multidrug resistant organisms, central line-associated bloodstream infections, and surgical-site infections.

Improving communication between members of the surgical team, staff, patients, significant others, and family members can help prevent wrong-patient, wrong-site surgery errors. The healthcare team should agree upon the correct procedure, the correct patient, and the correct site before any procedure. A licensed independent practitioner should make an obvious marking on the operative site before the procedure begins. A “timeout” should be called by an assigned member of the procedure team immediately before beginning each procedure or incision.

Competency in sedation is essential to avoid errors. Processes must be in place to ensure that experts in airway management, intubation, and advanced life support are quickly available in an emergency.

Deep sedation is a controlled state of depressed consciousness or a state of unconsciousness from which a patient is not easily aroused.

Moderate sedation is a drug-induced depression of consciousness during which patients respond purposefully to verbal commands, either alone or accompanied by light tactile stimulation.

Healthcare workers with advanced lifesaving skills have to be competent to administer and monitor sedation. Facilities should have measures in place in order to demonstrate that employees are competent.

A patient is considered recovered only when the patient has returned to the pre-procedural, pre-sedation state when it comes to their airway, breathing, circulation, and level of consciousness.

When patients are at risk of fall, put fall prevention strategies and protections in place that are customized to the individual patient's needs.

Risk factors for falls are associated with the patient's ability to move about, with or without the use of assistive devices.

Medication and visual impairment also contribute to patient falls. Most falls occur when a patient requires toileting. Call lights should always be within reach. Remind patients to use the call light if they need assistance.

Accrediting agencies require healthcare institutions to assess the potential of patient falls based on patient population and setting. A formal policy, which is monitored on a regular basis, should be put in place for those at risk.

To avoid mistakes, healthcare workers should focus on their tasks and avoid being rushed. Offer to help coworkers when they are involved in time-sensitive situations where distractions or shortcuts could lead to errors. Educate patients with face-to-face interactions and ensure understanding regarding care.

Screening people who may be at risk for suicide before or following discharge is an important step in patient care required by accrediting agencies.

Healthcare personnel have a duty to report to work rested and prepared. Fatigue is known to increase the risk of medical errors. The CDC reports that after 24 hours awake, cognitive impairment is similar to having a blood alcohol content of 0.1% — higher than the legal limit for driving in all states.

Healthcare personnel who "float" from one department to another may not have all the information necessary for all situations. So, be aware of how these floaters can increase the risk of errors. Accrediting agencies such as Healthcare Facilities Accreditation Program require all employees be able to perform the duties assigned.

Any suspicions of chemical impairment among personnel must be reported.

Do NOT report to work when ill, especially when running a fever. You risk transmitting your infection to patients and coworkers, and illness is known to cause fatigue and impairment of decision-making ability.

Personnel should be able to recognize and respond to changes in a patient's condition. They must be able to request extra help directly from specifically trained staff when a patient's condition appears to be declining.

Personnel should have adequate training and experience with medical equipment to avoid errors.

Employees should use effective hand-off communication procedures in all cases when patient care is transferred from one person to another, from one unit to another, or one institution to another. An article published December 4, 2013 in The Journal of the American Medical Association (JAMA) reported that a "handoff bundle" led to a significant reduction in medical errors and preventable adverse events among hospitalized children. TeamSTEPPS®, developed jointly by AHRQ and the Department of Defense, was one of the programs used to create the handoff bundle.

Reporting

All personnel have an ethical and legal responsibility to speak up about poor conditions regarding safe patient care. Healthcare leaders have a job to promote a culture of patient safety. They should promptly stop wrong personnel behaviors, including doctor behaviors that are known to increase the risk of medical errors. They should also support an environment where the focus is on finding a solution to reduce future risk of medical errors and NOT on blame.

If you are concerned about the safety or quality of care provided in your organization, follow your facility procedures for reporting those issues.

Medical errors and near misses must be reported as soon as they are discovered. You may report these concerns without disciplinary, retaliatory, or punitive action to your organization or the Centers for Medicare and Medicaid Services (CMS).

Module 4: Identifying and Reporting Abuse

Abuse: Mandatory Reportable Incidents

If you suspect a patient is suffering or has suffered abuse, neglect, or violence, you're responsible for ensuring his or her safety.

Types of abuse include physical, sexual, and emotional. All cases, even suspicions, must be documented and reported to the proper authorities following the procedures in place at your facility.

In most states, anyone who reports a suspected case of abuse in good faith is immune from criminal and civil liability. But if a mandatory reporter, which can include healthcare workers, teachers, and EMTs, among others, fails to do so, they could be charged with a crime. Know the laws in your state – some states require EVERYONE who suspects certain forms of abuse, to report their suspicions.

Certain injuries or diagnoses are mandatory reportable incidents. Some that commonly require reporting are shootings, stabbings, burn injuries, injuries caused by abuse or assault, certain sexually transmitted diseases, tuberculosis, HIV, and AIDS.

Child, elder, and domestic violence, abuse or neglect are mandatory reportable incidents in most states. Each state has its own mandatory reportable events and mandated reporters. It is VERY important that you know the laws in your state, and the procedures for reporting at your facility.

If you suspect a patient is being abused or neglected, talk to the patient in private, away from any suspected abuser. Assure the victim that they are safe. Even if probable excuses for the injuries are given, ask if anyone was involved in causing them harm.

Remember, each state has its own mandatory reportable events and mandated reporters, so learn what YOUR state requires.

The Centers for Medicare and Medicaid Services and accrediting agencies require that patients are safe from neglect and abuse. Also, most states do not exempt military medical facilities from complying with state reporting requirements.

Recognizing Abuse

It is important to know the signs and symptoms of abuse. Abuse occurs in every economic, cultural, and social group. Children, the elderly, and dependent people are especially vulnerable to abuse, but abuse occurs in all populations.

Physical abuse is the use of force to threaten or physically injure someone. Staff indifference to the infliction of an injury to a patient committed by an employee, visitor, or another patient is also considered physical abuse.

Signs of physical abuse may include: broken bones, sprains, dislocations, slap marks, pressure or restraint marks, and certain types of burns or blisters, such as cigarette burns, bruising in various stages of healing or clustered on only one body part, frequently the upper arms, patchy balding from hair pulling, black eyes, detached retinas, and missing teeth, imprint injuries -- marks that look like they were caused by a gag, fingers, or a belt.

Emotional and verbal abuse includes verbal attacks, threats, rejection, profanity, insults, and belittling acts that cause anguish, distress, and isolation. Public humiliation, degrading, name-calling, manipulations, and mind games are commonly seen emotionally abusive behaviors.

A patient suffering from emotional abuse may display rocking, head banging, or mumbling. Eating disorders and substantially lower than normal height and weight for their age can also be indications of emotional abuse. Also extreme developmental delays of speech and motor skills MAY be signs of emotional abuse. Withdrawing from normal activities, unexplained changes in alertness, or other unusual behavior changes can be signs of health problems in older people, but they can also be signs of possible emotional abuse.

Sexual abuse is sexual contact that is forced upon, or tricked or coerced from, someone who is defenseless or unable to give consent.

Torn, stained, or bloody underclothing may be signs that sexual abuse has occurred. Vaginal or rectal pain, frequent urinary tract infections, trouble walking or sitting, bruises around the breasts or genital area, unexplained sexually transmitted diseases, and a pregnancy in a dependent person MAY indicate sexual abuse. Sexual abuse is often difficult for a victim to talk about. As a healthcare professional it's your job to assure the victim that they're safe and there's no reason to be embarrassed.

When a caregiver fails or refuses to provide for a person's safety, or physical or emotional needs, it is considered neglect.

Common signs of neglect include poor hygiene, bedsores or untreated diaper rash, inappropriate clothing for the weather, an untreated injury or illness, or lack of proper immunizations. Excessive sunburn, insect bites, or frostbite could indicate possible neglect. Unusual and unexplained weight loss, malnutrition, or dehydration, could result from neglect. Other signs are unsafe living conditions, as well as begging for food or leftovers, and abandonment in a public place. Missing glasses, braces, hearing aids, walkers, or other adaptive equipment can indicate neglect or abuse.

Self-neglect results when a person cannot properly care for themselves.

Poor hygiene, changing behavior, and unsanitary living conditions may be signs of self-neglect. Reporting suspicions of self-neglect may lead to help for persons who are unable to care for themselves.

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER
HEALTH.EDU

Domestic violence is a pattern of abusive behavior that is used by one partner to gain or maintain power and control over another intimate partner. It can occur between married couples, family, roommates, or couples. Domestic violence can be emotional, physical, or sexual.

Behaviors a victim may exhibit are fearfulness, withdrawal, vague explanation of, or reluctance to say how an injury occurred, and seeming afraid to talk openly.

There are behaviors that might indicate someone is an abuser – a possible red flag would be a caregiver, or person close to the patient, who refuses to let you see the suspected victim alone. An abuser sometimes publicly insults or is dismissive of the abused party. It is common for the abuser to take over and speak for the abused person, and for an abuser to give a different explanation of how an injury happened.

In any of these situations, document and report as required by state laws and your facility's policies.