General Orientation AY 2023-2024
Compliance & Confidentiality in the Healthcare Setting

Healthcare is an expensive and complex business in the United States. Legislation and regulatory agencies have put a variety of safeguards in place to provide high-quality, affordable, and safe patient care.

In this module, you will learn about the regulatory agencies, key legislation, and guidelines for the healthcare industry related to quality patient care delivery and ethical business practices. We will also identify related practices that all healthcare workers must follow to comply with the various regulations.

Learning Outcomes:

1. Differentiate legislation and healthcare regulatory agencies that impact ethics and patient care in the healthcare setting.
2. Apply key concepts related to the confidentiality and security of health information.
3. **Clinical Healthcare Only**: Describe regulatory quality monitoring strategies that impact care delivery.
4. **Clinical Healthcare Only**: Apply care documentation strategies that support patient safety, regulatory mandates, and ethical care delivery.

Remember that learning outcomes will be the basis of the General Orientation Quiz if your role is required to complete a quiz.

Patient Care Partnership

Introduced by the American Hospital Association in the early ’70s, the Patient's Bill of Rights is considered foundational to many regulatory and compliance mandates that impact patient care today. In 2003, the Bill of Rights was renamed “The Patient Care Partnership” and a copy of these rights is provided to patients upon admission to a healthcare facility. Many other healthcare organizations such as clinics, physician’s practices, and rehabilitation facilities have adapted these rights for their specific environment.

Under the Patient Care Partnership, a patient should expect:

- High-quality hospital care.
- A clean and safe environment.
- Involvement in their care.
- Protection of their privacy.
- Help when leaving the hospital.
- Help with their billing claims.

Be sure to review the Patient Care Partnership document used in your assigned facility for additional expectations.

Corporate Compliance

The healthcare industry operates in a heavily regulated environment with a variety of high-risk areas. An effective compliance program helps mitigate those risks and contributes to providing patients with a safe environment and the highest quality care. In addition to the challenges associated with patient care, healthcare providers are subject to complex rules governing the coverage and reimbursement of medical services.

All healthcare facilities must have compliance plans based on these regulatory and legislative mandates that address ethical business practices. A Compliance Officer within the healthcare organization educates workers, routinely reviews healthcare practices for reporting violations to regulatory agencies, and initiates improvement or corrective processes. **Be sure to review the specific compliance policies and procedures for your assigned clinical facility!**

Healthcare Legislation

The primary goal of healthcare legislation is to protect patients and the integrity of healthcare funding. Spend some time reviewing the intent and impact of the key healthcare legislation using the links below!

False Claims Act

The False Claims Act covers fraud against the government based upon claims paid by any state or federal entity such as Medicaid or Medicare. Many healthcare professionals are not responsible for directly submitting claims for payment, but they can still contribute to false claims based on their documentation of care. Patient care documentation provides the basis for billing of services.

Common mistakes leading to false claims include:

- Documenting services or supplies that were not provided, and
- Failure to document Medical Necessity of treatments, diagnostic tests, medical devices or pharmaceuticals.

Anti-Kickback Statute

The Medicare and Medicaid Patient Protection Act, or the "Anti-Kickback Statute," allows criminal penalties to be implemented for knowingly and willfully offering, paying, soliciting or receiving anything of value to obtain a referral of a federal healthcare program. To avoid seemingly innocent practices that could lead to violations, most facilities have policies related to gifts and other rewards from patients, vendors, and healthcare-related organizations. As a healthcare worker, it is a good rule to never accept anything as an individual gift or reward for patient care. If in doubt, always ask.

Stark Law

The Stark Law is related to the Anti-Kickback Statute, in principle, since it specifically governs physician referrals for Medicare and Medicaid patients. Since physicians play a major role in determining what services a patient will receive, the Stark Law prevents patient referrals to entities where the physician has a financial interest, such as ownership, investment, or a compensation arrangement. This law includes any post-acute healthcare services that may be indicated such as physical therapy, occupational therapy, long-term care, hospice care, and so on. ***Patients should always be given a choice of providers for care or services.***

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was created to lower healthcare administrative costs, improve the efficiency and effectiveness of the healthcare system, and protect patient health information. HIPAA has had a major impact on healthcare providers and how patient information is handled in all healthcare environments.

HIPAA's Privacy Rule guarantees:

- Individuals the right to access their own medical information;
- The integrity, availability, and confidentiality of protected health information (PHI) will be maintained;
- Each healthcare facility must have policies and procedures that protect the use of all forms of PHI and control the release of PHI;
- Each healthcare facility must also have a designated Privacy Officer who is responsible for overseeing privacy and security practices; and
- Restricted disclosure of PHI based upon only what is needed. As a healthcare professional, you only have the "need to know" about a patient's PHI that is directly in your care.

We'll learn more about HIPAA and its impact on care a bit later in this program.

HITECH

The Health Information Technology for Economic and Clinical Health Act (HITECH) is a component of the American Recovery and Reinvestment Act of 2009. It strengthens privacy and security mandates for personal health information in these key areas:

- **Notification of Breach of Security for PHI:**
  Healthcare organizations and providers must notify affected individuals if they discover a breach of PHI.
- **Enforcement:**
  HITECH provides a tiered system for assessing the level of each HIPAA privacy violation and its related penalty.
  - Tier A - violations in which the offender didn't realize he violated the Act and would have handled the matter differently if he had. These result in a $100 fine for each violation up to $25,000/year.
  - Tier B - violations due to reasonable cause, but not "willful neglect." The result is a $1,000 fine for each violation up to $100,000/year.
  - Tier C - violations due to willful neglect that the organization ultimately corrected. The result is a $10,000 fine for each violation up to $250,000/year.
  - Tier D - violations of willful neglect that the organization did not correct. The result is a $50,000 fine for each violation, up to $1.5 million/year.
- **Health Record Access:**
  Organizations must provide the patient with an electronic copy of their file. The Act ensures that only a fee equal to the labor cost can be charged for an electronic request.
- **Genetic Information:**
  The Genetic Information Nondiscrimination Act (GINA) of 2008 prohibits health insurers and health plans from discriminating against beneficiaries based on genetic information. The HITECH Act clarifies that genetic information is protected under the HIPAA Privacy Rule and prohibits health plans (except for long-term care policies) from using or disclosing genetic information for underwriting purposes.

EMTALA

The Emergency Medical Treatment and Active Labor Act, or EMTALA, prevents hospitals from rejecting or refusing patients based on their ability to pay for services. EMTALA requires that all patients who present for care (including women in active labor) must be assessed through a medical screening examination. Until the patient's emergency condition has been established, no questions related to payment or proof of insurance may be asked.

EMTALA also requires specific documentation for transferring a patient from one facility to another, including the reason a transfer is indicated. Transfers are appropriate only if certain criteria related to the level of care are met and documented. If these guidelines are not met, fines can be up to $50,000 per violation for hospitals and physicians. In addition to fines, civil action can be brought by patients and receiving facilities to recover damages from personal injury or financial loss.

If you are working in the Emergency Department or caring for a patient that needs to be transferred to another facility, always refer to the related organizational policy.

Safe Haven

Most states have enacted legislation known as Safe Surrender or Safe Haven Laws that address infant abandonment in response to a reported increase in the abandonment of infants. The purpose of these laws is to ensure that relinquished infants are left with persons who can provide the immediate care needed for their safety and well-being. These laws focus on protecting newborns but have varying age limits from birth to 1 month old. **Hospital emergency departments are considered a Safe Haven and offer this service 24 hours a day.**

Regulatory Agencies

Four major agencies are responsible for monitoring the business practices and safety of the healthcare industry. These agencies include:

- The **Department of Health & Human Services** (DHHS) of the United States government oversees 300 programs such as the Food & Drug Administration (FDA), Medicare, Medicaid, & Public Health.
- The **Office of the Inspector General** (OIG) is an arm of the DHHS whose mission is to reduce fraud, waste, and abuse.
- The **Occupational Safety and Health Administration** (OSHA) regulates the occupational setting to maintain a safe environment for healthcare workers and the patients in their care.
- And lastly, the **Centers for Medicare & Medicaid Services** (CMS) administer the Medicare and Medicaid insurance programs. Focusing on quality activities, CMS oversees the regulation of laboratory testing, acute and intermediate care, nursing homes, home health agencies, and facilities for the mentally challenged. CMS also requires that healthcare organizations receiving Medicare/Medicaid payments, must be accredited by a CMS-approved agency.

Healthcare Accreditation

Healthcare organizations strive to maintain the highest standards when it comes to the quality of patient care delivery. These standards are derived from mandates from healthcare regulatory agencies and can also include additional organization-specific standards. Having an outside agency come into an organization to review the outcomes of these standards is known as the accreditation process. Successfully passing the review of these organizations is known as *accreditation*. Each organization and its professionals will have varying interactions with the Regulatory and Accreditation Agencies as a component of routine operations through data collection, reporting, event monitoring, and on-site surveys by the agency.

Several agencies can accredit healthcare organizations. These agencies may be discipline/service specific, such as an organization that just reviews laboratory services, or agencies that review all aspects of care delivery in a healthcare organization. The most used full accrediting agencies are:

- **The Joint Commission (TJC)** is a private organization whose mission is to evaluate healthcare organizations based on a stringent collection of standards related to safety and quality. MOST healthcare organizations use TJC.
- **Det Norske Veritas Healthcare (DNVHC)** was approved in 2008 as an appropriate agency to survey the safety and quality standards of healthcare organizations. There are a growing number of healthcare organizations choosing this agency for accreditation purposes.

Back to HIPAA … Everyone is Responsible for Protecting PHI

Based on the privacy mandates from HIPAA and HITECH, anyone who has access to or works with PHI is responsible for guarding the patient's privacy! This includes actual healthcare providers such as nurses, doctors, dietitians, lab techs, pharmacists, other healthcare professionals, and students in clinical rotations.

These mandates also include other non-clinical individuals who may have access to patient information such as volunteers, housekeeping, and any technical or support staff that encounters patients and/or patient PHI.

So What is PHI …

Protected Health Information (PHI) is ANY individually identifiable health information. This information may be in any form—written, verbal, and/or electronic. PHI falls into the following categories:

- An individual’s past, present, or future physical or mental health condition;
- The provision of health care to an individual; or
- Past, present or future payment for the provision of health care to the individual.

There are 18 HIPAA-specific identifiers:

1. Name
2. Address other than State
3. Dates related to an individual: birth date, admission date, discharge date, date of death, etc.
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical Record numbers
9. Health Plan numbers
10. Account numbers
11. Certificate or License numbers
12. Vehicle Identifiers
13. Medical Device identifiers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) numbers
16. Biometric Identifiers
17. Full-face photographic images
18. Any other unique identifying number, characteristic, or coding that is unique to the individual.

Paper PHI

Healthcare facilities are required to maintain reasonable practices and policies that safeguard patient PHI. Traditional paper PHI in the form of medical records or charts is stored in secure locations such as a nurses' station or the Medical Records department. By controlling location and access, paper records are protected from unauthorized release of PHI.

Other temporary forms of PHI, such as written notes, must be discarded in a secure manner. This is often done using a shredder or special trash container that is later bulk-shredded. Be sure to learn how your facility deals with paper PHI.

If you are a student, you should avoid using specific PHI in any documents, notes, worksheets, email, or any other communication. when completing care plans, concept maps, or other academic activities that include clinical content. You should not print or photocopy any component of the medical record. **Unauthorized printing or photocopying of PHI is considered a HIPAA violation and could result in serious consequences including dismissal from your program of study.**

Electronic PHI

Electronic PHI presents a challenge to protect. Policies and procedures that control how electronic PHI is accessed, stored, and protected must be in place. The use of passwords, biometric markers, and electronic signatures to protect electronic PHI is common practice. These electronic identifiers are designed to streamline, identify, and track activities within electronic healthcare records and other information systems where PHI is stored. Safeguarding these electronic identifiers is an important responsibility for all healthcare professionals, including students!

The use of computers at various points of care has created additional challenges for maintaining the security of electronic PHI. When accessing PHI in a patient care room or hallway, be sure to turn monitors away from others so casual viewing is obstructed. Privacy filters on screens are often used to minimize side-angle viewing of the screen.

Based on your responsibilities, you may be issued an electronic identifier that provides access to patient PHI. This identifier may be a username and/or password or a single sign-on, access token, or badge. Here are some key safety guidelines for maintaining electronic PHI integrity:

- Protect your usernames and passwords!
- Do not share your login information with anyone. Your login information is the same as your signature within the information system and tracks your use of any information system.
- Unauthorized logins or lost access tokens or badges should be reported immediately.
- Log off before leaving any computer workstation!
- If you find an unattended computer that is "logged in" under another healthcare professional's name, promptly log out before accessing any information.
- Lock computer systems in hallways or patient rooms when they are not in use.

Remember that while you may have access to more information than you need based on your role**, it is your responsibility to *__not__* access any information that you do not need to perform your assigned tasks. Unauthorized access can lead to serious disciplinary results and even legal action.**

Sharing PHI

Each patient is given a Notice of Privacy Practice document upon admission, and whenever services are provided, to explain their rights and how the facility may use or disclose their PHI. Individual patients must also know who has had access to their PHI. This is called "Accounting of Disclosure."

Sharing of PHI requires written authorization by the patient except for:

1. The purposes of treatment.
2. Billing purposes with insurance companies and medical offices.
3. Public interest and benefit activities such as:
   a. Public health initiatives to prevent/control disease, injury, or disability;
   b. As required by local, state, & federal law;
   c. Abuse or threats to health/safety; and
   d. Law enforcement purposes in some instances.

The release of sensitive PHI such as HIV status, alcohol and drug treatment, and psychotherapy notes may require additional written consent based upon state law and/or organizational privacy policies.

Communication Privacy

In the course of healthcare delivery, on-going communication between healthcare providers, support staff, patients, and their families and visitors must occur while maintaining patient privacy!

- Avoid discussing PHI in public areas such as hallways, elevators, waiting areas, and other public meeting spaces.
- Should you need to discuss a patient's condition with another healthcare provider in a public space, be sure to speak quietly and be aware that others may be nearby.

Using Communication Devices

A variety of communication technologies can be found in healthcare facilities to assist with patient care. HIPAA mandates apply to the use of these organizational technologies just as with any written personal healthcare information. **Be sure you know the use of communication technology policies for your assigned facility!**

ALERT: In most cases, personal phone or tablet use is prohibited in the clinical setting. This includes using these tools to take pictures or record audio or video.

The use of social media such as Twitter, Instagram, TikTok, and YouTube in the healthcare setting is prohibited to maintain patient confidentiality and prevent potential legal ramifications. You should NOT use ANY social media platform to communicate with other individuals about anything related to your work or clinical experiences.

While some healthcare organizations have embraced this technology for some patient and staff populations, most have not and have strict policies against this technology use.

Using these technologies will put you at risk for disciplinary action and/or liability for HIPAA-related fines.

Technology will continue to offer new communication tools that will require PHI to be guarded. Regardless of the communication tool or situation, protecting PHI should always be a guiding factor in your interactions with other professionals, patients, family, and visitors!

Family Members and PHI

Upon admission, most organizations will have patients identify whom to contact in a patient emergency and who is allowed access to relevant PHI. Some organizations use a code system consisting of a special word or number that must be used to release information to anyone other than the patient. This code may be used in person or over the phone. Always verify the identity of anyone requesting a patient's PHI to ensure they are authorized to have that information.

Family relationships can pose some privacy challenges. Although HIPAA regulations have been widely publicized, concerned family members may not always understand why you cannot release information about the patient. If you are communicating with a patient's family member, always follow the facility's privacy guidelines.

Dealing with parents & minors under the age of 18

Most of the time, PHI can be released to the parent of any patient under the age of 18, but some types of PHI will require the adolescent patient’s permission. Some examples of this type of PHI include birth control practices, STD status, pregnancy, substance abuse, and HIV status. Exact rulings are based upon state law, so be sure to verify what may and may not be discussed with parents without the adolescent patient’s permission. *Parents of adult patients must have the patient's permission for disclosure of PHI.*

Visitors during patient care delivery or procedures

Visitors, whether family or not, can pose an awkward situation during patient care delivery. Maintaining the patient's privacy is your responsibility and should guide your actions. Know who the patient has permitted to have access to PHI. If a visitor is in the patient's room and you need to deliver care that could compromise the patient's privacy, or discuss information with the patient that includes PHI, always ask the visitor to wait in the hallway or another designated area.

Privacy Patients

Sometimes patients will request to be a "privacy" patient. This means that even their name will not appear on any public listing of current patients such as a census report used for directing phone calls or visitors. Sometimes this is to prevent media from interfering with their care; but it could also be for domestic security or other reasons. Patients who have requested this level of privacy are appropriately protected from unwanted visitors and phone calls. If you are assigned to such a patient, it is critical you maintain their privacy from ALL inquiries - however seemingly innocent.

Reporting Confidentiality Breaches

Despite all the regulatory and confidentiality requirements healthcare organizations must follow, sometimes mistakes are made. Depending on the outcome of the mistake, varying levels of analysis and reporting are required. Reporting errors, confidentiality breaches, and compliance-related issues is a key responsibility of all healthcare professionals.

Depending on the situation, an incident report with appropriate follow-up by the Compliance or Privacy Officer and organizational leadership will be needed. Incident reports may be paper or electronic, and all healthcare workers should have access to complete these reports whenever they see, hear, or suspect a compliance or confidentiality issue.

Some examples of activities that are considered violations and should be reported include:

- Discussing confidential information in public areas.
- Looking at a patient's confidential PHI when not directly involved in the patient's care.
- Sharing a patient's PHI with an unauthorized person.
- Leaving paperwork with PHI unattended.
- Sharing an electronic identifier with another person - or - using someone else's electronic identifier.
- Storing electronic identifier information in an unsecured location.

Role-Specific Information:
Non-Clinical Health Care Professionals skip to the "Conclusion" on the last page of this document.
All other Healthcare Professionals, please continue with Quality Monitoring below.

Quality Monitoring of Patient Care Delivery

Quality improvement and reporting, which relate to compliance and regulatory guidelines, have become a daily consideration for care delivery practices in all settings. Several key quality initiatives impact patient care and require the diligent, consistent effort of all healthcare professionals. These initiatives are driven by the accrediting organization a healthcare facility uses and CMS. Most are interdisciplinary and are communicated to healthcare professionals in the form of policies and procedures. Patient care documentation and patient outcomes are the vehicles most frequently used for capturing compliance data. As a provider, you impact the quality of care your patients receive! Paying attention to your patient AND the details of care delivery will help you comply with the following quality improvement practices.

Performance Measures

Healthcare organizations choose performance measures based on their patient population and scope of care. The Joint Commission and CMS monitor these performance measures with a specific interest in "accountability" measures that have the greatest positive impact on patient care outcomes.

Outcome data for these measures are publicly reported and considered part of the accreditation process. Healthcare organizations choose their reportable measures based on their scope of care. You will learn more about an organization's specific performance measures in Facility Orientation.

Some of the suggested areas for Performance Measures include:
Assisted Living Communities
Cardiac Care
Emergency Care
Healthcare Staffing
Hospital-Based Inpatient Psychiatric
Immunizations

Palliative Care
Perinatal Care
Spinal Surgery
Stroke
Substance Abuse
Tobacco Treatment
Total Hip & Knee Replacement
Venous Thromboembolism

ISO and DNV

The basis of the DNV accreditation process comes from the standards identified by the International Organization for Standardization (ISO).   There are many ISO Standards that apply to the healthcare industry to control the rising healthcare costs without reducing the quality of care. The ISO 9001 standards support Quality Monitoring as an overarching standard leading to improving patient care delivery.

The key principles of ISO 9001 include:

- Patient & Care Team focus
- Clear Responsibility & Authority
- Involvement of people
- Process approach
- System approach to management
- Focus on continual improvement
- Improved internal and external communications
- Mutually beneficial supplier relationships
- Controlling outsourced processes

IHI Measures & Care Bundles

Many healthcare organizations use quality improvement strategies identified by the Institute for Healthcare Improvement (IHI). The IHI has identified a variety of measures that when implemented and monitored can lead to improved healthcare outcomes. By providing strategies to address numerous healthcare processes, the IHI has helped thousands of organizations improve outcomes.

The IHI's approach to clinical improvement processes identifies "care bundles" as a structured way of improving processes of care and patient outcomes. Bundles consist of a set of evidence-based practices — generally, three to five — that, when performed collectively and reliably, have been shown to improve patient outcomes.

In recent years, the IHI has identified specific patient care strategies for improving outcomes in several patient populations:

- Patients on Ventilators
- Patients with Central IV Lines
- Urinary Tract Infection Prevention
- Patients with Sepsis
- Patients with an AMI
- Patients with CHF

Patient Satisfaction

Patient satisfaction surveys have been around for years, but now CMS has initiated the Hospital Consumer Assessment of Hospitals and Health Systems, or HCAHPS (pronounced H-caps), to capture opinions from patients on critical aspects of care. The results of these surveys are tied to reimbursement for the hospital and are publicly reported on the Hospital Compare website. ALL care providers can impact the outcomes of these surveys – including students!

There are several summary measures captured by the survey:

- How well do care providers communicate with patients?
- How responsive are care providers to patients' needs?
- How well do care providers help patients manage pain?
- How well do the care providers communicate with patients about medications?
- Was key information provided at discharge?
- How is the cleanliness and quietness of patients' rooms?
- What is the overall rating of the hospital, and would they recommend the hospital to family and friends?

Hospital Acquired Conditions (HACs)

As an outcome of quality monitoring, CMS and many third-party payors no longer reimburse organizations related to the care required for preventable conditions not present on admission. When these HACs occur, they often result in the need for high-cost services for which the organizations cannot recover charges. Absorbing these costs can lead to poor financial performance over time which can lead to an organization closing its doors.

Current HACs include:

- Retained foreign object after surgery
- Air embolism
- Blood incompatibility
- Pressure ulcers (Stage III, IV)
- Falls and trauma
- Catheter-associated urinary tract infection
- Vascular catheter-associated infection
- Poor glycemic control such as diabetic ketoacidosis, hypoglycemic coma, etc.
- Surgical site infection after specific cardiac, orthopedic, and bariatric procedures
- Deep vein thrombosis/pulmonary embolism (DVT/PE) following total knee or total hip surgery
- Iatrogenic pneumothorax following venous catheterization

Sentinel Event Analysis

Unfortunately, in healthcare settings, things sometimes go wrong. A sentinel event is an unexpected occurrence involving death or serious physical or psychological injury of a patient, or risk thereof. It is called "sentinel" because it requires immediate investigation and response. The terms "sentinel event" and "error" are not synonymous; not all sentinel events occur because of an error, and not all errors result in sentinel events.

Accredited healthcare organizations are expected to identify and respond to all sentinel events. The organization's response should include the following: conducting a timely, thorough, and credible root cause analysis; developing an action plan to implement improvements to reduce risk; implementing improvements; and monitoring the effectiveness of improvements.

Some examples of sentinel events are:

- Patient suicide
- Unanticipated death of a full-term infant
- Abduction of any patient receiving care
- or services
- Physical Assault or Homicide of any patient, staff, or visitor
- Discharge of infant to the wrong family
- Maternal death or morbidity
- Sexual abuse/assault of patient, staff, or visitor
- Hemolytic transfusion reaction involving administration of blood or blood products having major blood group incompatibilities.
- Surgery/procedure on the wrong patient/body part
- Unintended retention of a foreign object in a patient after surgery or other procedure
- Medication error resulting in permanent or severe harm
- Delay in treatment
- Patient fall resulting in any fracture or surgery, leading to permanent or severe harm
- Patient death/injury while in restraints
- Infection-related event
- Fire

Documentation of Care

Regulatory compliance and patient care outcomes are based on the medical or health record of patients. This document, whether paper or electronic, is also the foundation for communicating patient care delivery and patient safety. As you contribute to these records, here are some concepts and practices to keep in mind:

- The medical record is a legal document and all entries must be dated and signed, either physically or electronically, by the author.
- Entries into the document should be accurate and reflect the patient's plan of care, services provided, response to care, and ongoing health status. Content should reflect compliance with regulatory standards of care and organizational policies.
- If you make a documentation error, follow organizational procedures for correcting the error. This will vary based on the type of medical record an organization uses. Simply erasing or deleting the error is not acceptable.
- Always remember that the medical record is confidential, and it is your responsibility, along with the healthcare organization, to protect it from loss, tampering, and unauthorized use or disclosure. Access to this document should always be on a "need to know" basis.

Tips for Error-Free Documentation

Healthcare organizations may employ a variety of documentation strategies, so be sure to review the documentation practices of your facility prior to documenting patient care.

- Always make sure that you have accessed the correct patient’s record before documenting, to prevent documentation or charge errors!
- Review the orders of your patients to make certain that the supplies you use and the care you provide are covered by a medical order.

- If you find that services are needed or being provided without an order, immediate steps should be taken to obtain an order to prevent a fraudulent medical record.
- If you find an order that is not clear, obtain clarification from the physician or practitioner before initiating the order.
- Document care provided at the point of care whenever possible. Your documentation serves as communication with other healthcare professionals for ongoing continuity of care – often in real-time.

Medical Necessity:

Medical necessity is generally defined as providing services or care that is "reasonable and necessary" considering clinical standards of practice and is a direct order from a physician or practitioner. Even if a service is reasonable and necessary, Medicare and other insurance coverage may be limited if the service is provided more often than allowed or not within a clinically accepted standard of practice. Regulatory mandates require that a rationale be recorded for any diagnostic study, procedure, supply, or medication that is not recognized as a standard of practice for a given diagnosis. **Failure to document medical necessity is considered another form of fraud.**

How does Medical Necessity impact healthcare professionals?

In Paper Medical Records:

Medical Necessity is often challenged by insurance and quality monitoring long after the care of services has been provided. It may be the responsibility of the pharmacy, radiology, or other healthcare professionals to flag any questionable or unclear orders. If necessity is not updated, reimbursement for the medication, procedure, etc. will not be collected by the healthcare organization resulting in a loss of revenue.

In EMRs:

In electronic medical records (EMRs), questions about medical necessity are often presented at the point of care. An Advance Beneficiary Notice or ABN is used to alert healthcare professionals when medical necessity is questioned for a particular study or medication. This alert offers care providers an option to document the need more completely for the care or service. The alert also offers patients an opportunity to share in the decision-making process related to the financial responsibilities they may incur should reimbursement not be provided by third-party payers.

If your patient has an ABN showing in their EMR, follow the organizational policy to determine the appropriate next steps. IF you have any doubts about an order - ALWAYS clarify the order before implementation.

Advance Care Planning

Another key component of ethical patient documentation is related to advance care planning. A reality of the healthcare environment is that a patient's health status can radically change and require decisions to be made about their continued care. Advance care planning by the patient involves learning about the types of decisions that might need to be made and then letting others know about any preferences they may have. These preferences are communicated to the healthcare team by putting them into an advance directive which becomes a component of the patient's medical record.

There are several components of advance care planning:

- Selecting a **Durable Medical Power of Attorney** for healthcare allows a patient to name a "patient advocate" to act for and carry out the patient's wishes if they become unable to participate in decision-making related to their care.
- Completing a **Living Will** in which the patient states their wishes for end-of-life care in writing.
- A "Do Not Resuscitate," or **DNR**, request alerts healthcare professionals that no CPR is desired should the patient become unresponsive and experience a cardiopulmonary arrest. The "Do Not Intubate," or **DNI**, request alerts healthcare professionals that no intubation or mechanical ventilation is desired.
- Decisions about **Organ and Tissue Donation**. Typically, the heart, lungs, pancreas, kidneys, corneas, liver, and skin are donated but this can be specified as desired by the patient and/or medical condition.

These requests must result in a written order by a physician based upon these advance directives or the reasonable expectation that the patient is terminal and would not benefit from advanced life support strategies.

As a healthcare professional or student, it is your responsibility to know the resuscitation status of patients in your care so you can respond appropriately should the patient have a change in status.

Organ Donation

The National Organ Transplant Act passed in 1984 provides the basis for all regulations related to organ donation and transplantation. A variety of federal and state agencies oversee the complex donor and transplant process. Since it is possible for a single donor to save up to eight lives, any pre-determined donor status is typically identified for patients as a part of the intake process.

Should a non-donor patient's medical status deteriorate, patients/families should NEVER be approached about organ donation except by a clinician who has been trained to have this type of conversation. Each healthcare organization will have a designated team to assist with patients/families seeking organ donation.

If you are confronted with an opportunity for a patient to become an organ donor, reach out to your supervisor to follow the prescribed process for obtaining permission/donor status.

CONCLUSION:

Healthcare is a complex and high-risk environment that demands compliance with regulatory and organizational policies and practices to ensure a safe environment for patients. Equally important is maintaining the confidentiality of patients within the healthcare system.

All healthcare professionals - workers and students - are charged with maintaining patient confidentiality, ensuring medical records are accurate and reflective of health status, and applying ethical care delivery and business practices in daily operations.

If you have any specific questions related to compliance and confidentiality practices, please talk with your supervisor!

Remember that there will be content from this material and opportunities to apply what you've learned in the General Orientation Quiz!