Privacy, Dignity, and Confidentiality

Caredemy

Online Training Academy

Course Name:

Privacy, Dignity, and Confidentiality

Course Description:

This course will give an overview of how health and social care workers can support the privacy and dignity of those in their care. U.S. confidentiality legislation will also be covered.

Course Learning Objectives:

At the end of this course, the learner will be able to:

- Understand principles of privacy and dignity in health and social care
- Describe ways to maintain the privacy and dignity of others when providing care
- Understand why it is important to maintain confidentiality
- Describe how individuals have rights to make choices about their care
- Understand how risk assessment processes can support the rights of individuals to make their own choices

Course Requirements:

Participants must complete all learning modules and pass the multiple-choice course assessment.

Privacy and Dignity

When privacy and dignity are not respected, individuals feel:

- Ignored and unimportant
- Exposed or vulnerable
- That the staff doesn't care what happens to them
- That they are a nuisance to the health and social care staff
- Uncomfortable, embarrassed, in pain, or distressed
- That their preferences don't matter
- Angry when private details are revealed to those who do not need to know them
- That they do not have control over what happens to them

Maintaining privacy and dignity affects the care experience and undermines a person's individuality.

Importance of Privacy and Dignity

Staff should be aware of how their behavior might harm a person's privacy and dignity. Health and social care staff should be aware of:

- The environment in which they provide care
- The processes they use to provider care or keep and/or discuss personal information
- How behavior can harm another's privacy or dignity

Privacy: Privacy is about making sure a person feels cared for and that their information is confidential and safe.

Dignity: Dignity is seeing someone as an individual and respecting them and their way of life.

Best Practices

Maintaining privacy and dignity means being caring, kind, and compassionate. Some mistakes that people make can be subtle but make a big difference to the person receiving care.

Raising Concerns: Health and social care staff have a duty of care to those who receive services the organization provides. If you have concerns about how dignity and privacy at your organization, you can:

- Talk to your manager
- Talk with the colleague in question
- Discuss concerns with the person's family
- Report concerns to local authorities

Maintaining Dignity: Staff must respect a person's right to refuse treatment. The person should feel empowered and included in their care decisions.

Information Governance

Health and social care staff often have access to large amounts of confidential data. It is important that staff apply the principles of information governance in their daily work. There are both simple and complex methods for maintaining proper information governance. Maintaining a patient's confidentiality is the staff's legal and ethical duty.

Six Caldicott Principles

The six Caldicott principles that support confidentiality in health and social care are:

1. Justify the Purpose: every proposed use or transfer of patient identifiable information within or from an organization should be scrutinized and clearly defined.
2. Do not use patient identifiable information unless absolutely necessary.
3. Use the minimum necessary patient identifiable information
4. Access to patient identifiable information is on a strict need-to-know basis.
5. Those with access to patient identifiable information should be aware of their responsibilities.
6. Health and social care workers must understand and comply with the law.

Keys to Keeping Data Secure

To keep data secure, you should:

- Use strong, secure passwords
- Use security codes and do not share them with unauthorized individuals
- Use encryption software when needed for sensitive data, such as electronic patient records
- Lock drawers, cabinets, and doors.

Strong passwords contain:

- No personal information that is easily guessed
- Numbers and a mix of upper and lowercase letters
- Characters such as full stops or asterisks

Patient Notes

Patient records should:

- Be factual, accurate, consistent, dated, and signed in pen so notes cannot be erased
- Have alterations and amendment must be timed, dated, and signed
- Be Written in a way to ensure they are readable
- Not include too much medical jargon, offensive comments, personal opinions, or unconventional abbreviations
- Include medical observations such as test results, diagnoses, and prognoses

Destroying Records

Your organization should have guidelines regarding how records and notes should be destroyed. Ask your information governance lead if you do not know your organization's policies and procedures for safe destruction of notes and records.

Social Media

It is vital that health and social care workers are aware of how they utilize social media as it may affect the security of sensitive information they come across as part of their daily work. This could be posting about your job and having a person comment that a patient is lucky to have them, divulging information about the person being treated, posting about the organization in a way that reveals information that should only be communicated internally, or posting images from work where confidential information is in the background.

Social Media Guidelines

Before you post on social media, consider:

- Is my place of work identifiable?
- Are my colleagues identifiable?

- Are those that I care for identifiable?
- Will my post bring my organization or profession into disrepute?
- Will my organization or manager be happy with my post?
- Are any security details such as passwords or passcodes identifiable?

Protecting Client Privacy: Understanding HIPAA

HIPAA, which stands for the Health Insurance Portability and Accountability Act, is a crucial legislation introduced in 1996. It aims to ensure the confidentiality and privacy of personal, financial, and health information belonging to clients.

This act imposes strict guidelines on healthcare organizations, including medical offices and hospitals, to safeguard sensitive data. For instance, HIPAA mandates measures such as ensuring that computer screens displaying patient information are not located in high-traffic areas where unauthorized individuals might inadvertently view confidential details.

Understanding the Importance of Confidentiality in Care

The Privacy Rule, implemented on December 28, 2000, establishes federal protections for patient health information, granting individuals rights over who can access their data and how it can be utilized.

Confidentiality is the cornerstone of trust and privacy, ensuring that sensitive information remains secure and undisclosed.

What Caregivers Should Know About HIPAA: Clients receiving care services may possess medical records and instructions from their healthcare providers, including details about medications. It's crucial for caregivers to understand that this information is strictly confidential, and they are prohibited from sharing it with anyone outside of those directly involved in the client's care.

Protecting Confidential Information in Care

In the realm of care, safeguarding personal information, often referred to as Protected Health Information (PHI), is paramount. Given the intimate nature of the caregiver-client relationship, it's natural to encounter personal details about the person's family and friends. It's imperative to maintain strict confidentiality regarding any information disclosed by the individual or heard during the course of caregiving duties.

Just as company information remains confidential in any workplace, a client's personal information must be treated with the utmost discretion.

For instance, if you learn that a client has a terminal illness, it's crucial not to disclose this sensitive information, even if a family member or visitor brings it up.

Financial Privacy

Financial matters pertaining to a client should be treated with sensitivity and confidentiality. Seniors, particularly, may feel particularly vulnerable discussing financial issues, as many rely on fixed incomes. Caregivers should refrain from sharing their own financial concerns and gently redirect conversations if a client broaches the topic.

Additional Guidelines:

- Refrain from sharing a care client's information with third parties.
- Always verify the identity of healthcare providers contacting you on behalf of the client before sharing any information with them.
- Avoid involving yourself in the transfer of information to medical professionals to protect both yourself and the client's privacy.
- Never engage in financial transactions with a senior client to ensure the safety and well-being of both parties.
- Remember, personal information shared by a client remains confidential and should be treated with the utmost respect and discretion at all times.

Protecting Individually Identifiable Health Information under HIPAA

HIPAA, the Health Insurance Portability and Accountability Act, plays a crucial role in protecting sensitive health-related details. This includes information related to a person's medical treatment, reasons for clinic visits, and participation in Medicaid programs designed for low-income individuals.

Examples of such protected information encompass personal identifiers like names, addresses, social security numbers, medical record numbers, or even photographs associated with the individual.

Protected Health Information (PHI) encompasses all individually identifiable health data, regardless of its format—be it in written, verbal, or electronic form. This includes information stored on paper, computers, electronic devices, or even in the caregiver's memory.

Exceptions to the Rule:

Certain employment and education records fall outside the scope of HIPAA regulations. Under HIPAA, caregivers are granted access to only the minimum necessary PHI required to fulfill their job responsibilities. Moreover, they are authorized to disclose the minimum necessary information when responding to requests, ensuring that confidentiality is maintained at all times.

Exceptions to the Minimum Necessary Rule:

- Disclosures or requests for treatment purposes by healthcare providers.
- Uses or disclosures authorized by the client or participant.
- Disclosures mandated by law or to the Secretary of HHS.
- Disclosures required by law.

By adhering to these regulations, caregivers uphold the integrity of PHI and contribute to maintaining the privacy and security of individuals' health information.

Verification Protocols

Prioritize verifying the identity and authority of individuals seeking access to information. Ensure thorough documentation of each request by recording the person's name, contact details, and the timestamp of the interaction to demonstrate proper verification procedures.

Guidelines for Permission to Access Protected Health Information (PHI) and TPO:

Treatment, Payment, Operations

- Authorization is typically not required before disclosing a care recipient's PHI for purposes related to treatment, payment, or healthcare operations.
- TPO encompasses activities such as quality assessments, medical reviews, auditing, planning, and budgeting within the healthcare realm.
- For Abuse Reports and Investigations

In most cases, specific written authorization from the client or care recipient is necessary before using or disclosing their PHI for purposes beyond treatment, payment, or operations (unless permitted by the Privacy Rule).

Breaches in Confidentiality

Situations which could lead to violations of confidentiality are:

- Discussing work with family and friends
- Informal discussions with colleagues
- Social gatherings
- Incoming phone calls
- Attentive repairman

Noncompliance with HIPAA: Legal Consequences

It's crucial to adhere to HIPAA regulations as failing to comply constitutes a violation of federal law, potentially resulting in fines or imprisonment for offenders.

If you become aware of any violations of HIPAA requirements, it's your responsibility to promptly report the situation to your manager or supervisor to ensure legal compliance. Employers are obligated by law to safeguard employees from harassment or retaliation for reporting suspected privacy breaches.

Law Enforcement Interaction

There are instances where disclosure of Protected Health Information (PHI) to law enforcement is permissible without the client's authorization. This includes situations where the PHI pertains to an individual suspected of criminal activity, and the disclosed information is limited to details necessary for identifying the suspect and understanding any related injuries.

When in doubt about handling private health information in any scenario, always consult your supervisor for guidance.

Remember, refrain from discussing PHI witnessed or heard during your job duties with anyone unless absolutely necessary to maintain confidentiality and uphold legal obligations.

Understanding HIPAA: Who's Affected?

HIPAA regulations extend to both Business Associates (BAs) and Covered Entities (CEs).

BA: A Business Associate (BA) encompasses individuals or entities involved in activities granting access to health information, either through performance or assistance.

Covered Entities (CEs) include:

- Caregivers
- Healthcare Clearinghouses
- Healthcare Providers engaged in electronic transmission of health information for standardized transactions approved by the Health and Human Services, such as hospitals, medical centers, senior home care agencies, doctors, and nurses
- Health Plans

These entities are all subject to HIPAA requirements, ensuring the protection and privacy of health information in their operations.

Protecting Client Information: A Caregiver's Responsibility

Example 1: Let's say you accompany your client, "Mary," to a doctor's appointment and learn about her deteriorating health condition. Despite knowing this, Mary chooses not to disclose the diagnosis to her daughter during a subsequent visit. As a caregiver, you must respect Mary's decision and refrain from sharing any confidential health information with her daughter or anyone else. Just like attorney-client confidentiality, where lawyers are bound to keep information private, you are similarly obligated to maintain the confidentiality of Mary's diagnosis.

As previously discussed, this sensitive information falls under the category of Protected Health Information (PHI). Other details you must not disclose include past, present, or future health conditions and payment for healthcare services.

Example 2: In another scenario, let's say you discover that Mary has Stage 1 Alzheimer's Disease, yet she opts not to share this with anyone. When her neighbor questions Mary's forgetfulness, you cannot reveal her medical

condition. It's essential to respect Mary's privacy and refrain from disclosing any sensitive health information to third parties.

Understanding HIPAA Regulations

PHI includes medical records, laboratory reports, or hospital bills containing a patient's identifying information.

The Security Rule establishes standards for securing electronic Protected Health Information (ePHI).

The Breach Notification Rule mandates that Covered Entities (CEs) and Business Associates (BAs) must report any breaches or unauthorized access to confidential information.

The HITECH Act: Enhancing HIPAA with Modern Measures

In 2006, the HITECH Act was introduced as an amendment to HIPAA, aiming to bolster the security and efficiency of healthcare information systems. Part of the broader American Recovery and Reinvestment Act of 2009 (ARRA), the HITECH Act significantly raises the stakes for non-compliance with regulatory standards.

The primary objective of the HITECH Act is to expedite the adoption of Electronic Health Records (EHR) systems across healthcare providers. This shift towards digital records is intended to streamline healthcare processes and improve patient care outcomes.

What Does this Entail?

Mandated Use of Electronic Health Records: The government encourages all healthcare providers to transition to Electronic Health Records for improved efficiency and accessibility.

Enhanced Security Measures: Stricter security protocols must be adhered to, ensuring the protection of sensitive patient information.

Increased Legal Liability: Non-compliance with the new regulations carries heightened legal consequences, potentially leading to significant liabilities for organizations.

Government Enforcement: The government possesses greater authority to enforce compliance with the new rules, enabling the imposition of fines on non-compliant entities.

Risks of Using Unsecured Devices

As discussed earlier, the HITECH Act, a component of HIPAA, imposes stringent regulations on the storage and transmission of healthcare information. These regulations encompass specific encryption protocols, storage requirements, and even necessitate costly insurance coverage for companies engaged in Electronic Health Record (EHR) management.

- Sending emails about your client using your personal computer—NOT SECURE
- Posting about your client on Social Media—VIOLATION of HIPAA
- Texting your manager about a client's care details—VIOLATION of HIPAA

Sending sensitive information via unsecured platforms like text messages or using personal devices for work-related communications poses a significant risk of breaching patient confidentiality and violating HIPAA regulations. It's imperative to adhere to secure communication channels and maintain the privacy and integrity of client information at all times.

Expiration of HIPAA Authorization Forms

Have you ever wondered why you have to repeatedly sign HIPAA forms at the doctor's office? It's because these authorization forms have expiration dates. When your agency begins providing care to a new client, they obtain consent from either the client or their authorized representative to access their health information. However, it's illegal for the agency to access Protected Health Information (PHI) after the expiration date of these authorization forms.

For example, if Rose initially signed a HIPAA form for a 6-month care period but continues to receive care into her second year, the agency must ensure that they have current, non-expired authorization forms on file.

What if a client refuses to sign a HIPAA form? Despite their refusal, they cannot be denied access to care, and the agency/provider must still adhere to HIPAA standards. However, the agency will keep a record on file indicating that the client/patient refused to sign the form.

Advance Directives

Advance directives are documents that specify the type of treatment individuals desire or reject under severe medical conditions. These documents are utilized when a person is unable to communicate their wishes. They provide written evidence of an individual's preferences, preventing families from having to guess their desires. Expressing one's wishes in advance benefits everyone involved. It spares family members from making difficult decisions during what is likely one of the most stressful times of their lives. It also ensures that physicians know whose instructions to follow if the family disagrees about the medical treatment the individual wants. There are generally two types of advance directives:

Living will: A legal document that details the medical care an individual wants or does not want if they become incapable of making decisions. An example would be the use of a feeding tube.

Durable medical power of attorney: A legal document that appoints another person to act as an agent or surrogate in making medical decisions if the individual becomes incapable of doing so.

Individuals can complete advance directives themselves. While the writing does not need to be done by a solicitor, it must be completed while the person is still competent. In some states, these forms do not need to be notarized. However, if the individual moves to a state that requires notarization, the forms would be invalid.

Do Not Resuscitate Order (DNR)

The Pre-Hospital Medical Care Directive, commonly known as the "orange form" or a DNR, is a specific type of advance directive. This form indicates that if the individual's heart stops beating or they stop breathing, they do not wish to receive cardiopulmonary resuscitation (CPR) under any circumstances. The bright orange color of this form ensures that paramedics and emergency medical services personnel are aware of this decision.

1. Agency-Specific Policies and Procedures

The policies and procedures for honoring an orange form can differ between agencies. Some agencies have policies requiring the Direct Care Worker (DCW) to administer CPR (if certified) regardless of the presence of an orange form. Other agencies have specific procedures in place for situations where the individual

has a valid orange form. When a DCW observes that the consumer has an orange form, they should contact their supervisor to understand the applicable policies and procedures regarding CPR for that consumer.

It is also crucial to remember that the orange form only pertains to cardiac and respiratory arrest. If the consumer experiences a different type of medical emergency, the DCW should provide first aid and call 911 as necessary.

2. Display of the Orange Form

Given the urgency of emergency medical situations, the Pre-Hospital Medical Care Directive must be prominently displayed so that paramedics can easily see it in the event of cardiac or respiratory arrest. Recommended locations include on the refrigerator, behind the front door, or behind the living room door.