# ICD-11 MMS Education Tool

# Confidentiality and ethics

## Contents

* Confidentiality
* Privacy
* Authorisation
* Security
* Avoidance of potential harm
* Breaches of confidentiality

## Confidentiality

Confidentiality refers to the obligation of not disclosing data about information delivered in confidence to unauthorised third parties. This duty was codified in the Hippocratic Oath in the 4th century BCE and is still one of the core principles of medical ethics.

National legal frameworks, state and local regulations, and institutional guidelines provide specific rules and information regarding how to maintain confidentiality.

### Your duty to maintain confidentiality

Confidentiality with regard to information about a person in health settings rests in the notion that the person shared this information with health professionals with an explicit or implicit understanding that this data would not be revealed to anyone else not authorised to have that information.

You have access to this privileged information on the understanding that you will respect confidentiality and will not share this information with unauthorised parties.

It is important to note that information does not become ‘non-confidential’ when a person agrees to allow someone else to view it; nor does this compromise the duty to uphold confidentiality.

### Why is confidentiality important?

Maintaining confidentiality benefits the public by reinforcing patient confidence that when revealing personal information to relevant professionals and staff, the information will be protected and not shared with people who should not have access.

This improves the quality of health information because people may be more willing to share all relevant information if they trust it will be handled in a confidential manner.

## Privacy

Privacy relates to protecting an individual’s control over what personal information and decisions may or may not be shared with others.

For instance, when a physician examines or speaks with a patient it is usually done in a non-public area so that the information exchanged cannot be heard by anyone else.

### What is the difference between confidentiality and privacy?

The terms confidentiality and privacy are often used in the same way. However, they are different.

Confidentiality is the obligation of professionals and other health workers not to disclose information about people to unauthorised third parties.

Privacy relates to protecting an individual’s control over what personal information may or may not be shared with others.

Confidentiality refers to information and we speak of a ‘breach of confidentiality’ whereas privacy pertains to people and we speak of a ‘loss of privacy’.

It is important to note that different cultures and communities will have different concepts of what an individual’s right to privacy means, and what levels of confidentiality they expect. Accordingly, always make sure you are aware of your local and national rules and regulations.

## Authorisation

Authorisation is the granting of permission to view confidential information. It can be expressively granted by a patient, or be implied, as for medical staff that are directly involved in the patient’s treatment, or to a facility or institution where the data could be analysed for research or other purposes.

Any information that might allow the identification of a specific person should only be viewed by people who are authorised to do so.

Authorisation means that a person is legally permitted to look at the information. For example, medical staff, coroners, and coders are all people who can be authorised to see sensitive information.

### Authorised user

The **authorised user** is the person who requests the use of confidential information.

* The authorised user must only use the information for appropriate authorised purposes, and must return the information as required.
* The user must not attempt to gain access to information which they are not authorised to view.

For example, a coder has authorisation to view a person’s medical or death record, however they can only use this information for morbidity or mortality coding. Discussing or revealing this information in any other circumstance unrelated to their job is considered a breach of confidentiality.

### Authorised supplier

The **authorised supplier** of confidential information must verify that the requesting person is an **authorised user** and determine their level of authorisation.

The supplier must be aware of the level of information that can be made available to the authorised user and take appropriate steps to guard against unauthorised disclosure.

For instance, an authorised person may have limited access that allows them to view and record a person’s date of birth, sex, marital status, and address. However, they may not have authorisation to access information regarding HIV test results.

## Security

Authorised users must guard against unauthorised access to confidential information. This means that users must secure the information and any recording of that information in a way that prevents unauthorised viewing.

### How can we ensure confidential information is secure?

One primary way to minimise risk is to only gather information that is materially relevant or necessary. For health care providers this means only gathering information that is necessary for the treatment and diagnosis of their patients. For coding and epidemiological work, we should only collect information that is needed to complete the required documentation or study.

### Safeguards for physical files

Simple safeguards can be utilised by health professionals, coders and researchers to guard against confidentiality breaches. Confidential information that is contained in paper files and physical form can be protected by:

* Restricting physical access to unauthorised users only
* Only releasing information that the user is authorised to access, and maintaining a written record on file with the approval for the release of information
* Storing information in a location that requires authorised access
* Safeguarding information when transporting from one location to another
* Use authorisation and release of information forms that require signatures when physically accessing the information
* Require all information be reviewed in-house and not removed from the institution or organisation to control the risk of the information being misplaced, lost or accessed by unauthorised people
* Secure disposal and destruction of medical files and documentation in a proper manner that prevents unauthorised access

While some health care systems still operate with the pen and paper style of documentation, increasingly information is stored in an electronic format. The ICD-11 is intended for coding in an electronic environment, even though it is used as an analogue printed version in some countries.

### Safeguards for electronic files

For information stored in an electronic format, data can be protected using the following methods:

* Username and password authentication
* Limiting electronic access to data to users that have been assigned permission by the relevant authority
* Secure wireless networks
* Computer monitor privacy screens

### De-identifying information

Another way to protect data is through de-identification. This is the one way to make data accessible to other professionals who possess lower authorisation levels.

De-identification is the process of removing person-identifiable information from the data so that it is impossible to identify who the information refers to given only the de-identified information.

Person identifiable information includes:

* Name
* Address
* Telephone numbers
* Email addresses
* Social security or national identity numbers
* Medical record number
* Health insurance number
* Month and day of dates that related to the person, such as date of birth and death, admission and discharge dates
* Photographs
* Finger prints

## Avoidance of potential harm

A person may suffer ‘harm’ physically, socially, or psychologically as a result of a breach of confidentiality. The disclosure of sensitive information can potentially lead to stigma and discrimination against an individual.

Conversely, greater harm can result from maintaining confidentiality than from not doing so. Some circumstances may require a judgement that involves balancing the harms to, against the interests of, the patient, deceased person and other relevant parties. For instance, the nondisclosure of one person’s confidential information may result in another individual or a community being at risk of developing a harmful condition or being exposed to a harmful situation.

You may have to share information against a person’s wishes. This is usually when required by legislation, statutes, regulations or the court. For example to report certain communicable diseases, or suspected neglect or maltreatment.

## Breaches of confidentiality

A breach of confidentiality is a disclosure via any means, intentional or not, to an unauthorised person. This can be by direct disclosure to an unauthorised party, or not adequately securing the confidential information as to allow unauthorised parties to access it.

The exception would be in instances where a person is required by legislation, statute or regulation to report or disclose confidential information, it is not appropriate to refer to that as a ‘breach of confidentiality’.

The means of the disclosure can be:

Verbal

* By direct disclosure to an unauthorised party
* Speaking where unauthorised parties can overhear your conversation, such as in a public area
* Talking on a wireless headset that could be eavesdropped on

Visual

* By allowing an unauthorised party to read the information or read your record of the information
* Sending or emailing the information to an unauthorised party