***Training Materials on the International Protocol***

**PART V MODULE 13 – STORING AND HANDLING INFORMATION**

**Session objectives:**

By the end of the session, participants should be in a position to:

* Understand the obligation to safely handle and store information
* Recognise that storage limitations have implications for collection of information
* Identify the different legal and other requirements for physical, digital and forensic evidence

**Suggested duration of session:**  60 to 90 minutes

**Exercise:** None

**Relevant sections of International Protocol:**

Pages 202-209; Module 7 – Do No Harm; Module 8 – Safety and Security; Module 9 –Planning; Module 10 – Types of Evidence of Sexual Violence; Module 11 – Interviewing; Module 12 – Collecting Additional Information; Annex 4 – Sample Sexual Assault Medical Certificate; Annex 9 – Chain of Custody Form

The trainer for this module should have professional experience dealing with witnesses and evidence in an investigation or documentation context, and should ideally have specific expertise in information storage and management. This is the last module of Part V of the Protocol – Documentation in Practice: Gathering Information, and it brings together numerous issues from the previous modules – Do No Harm, confidentiality, risk assessments, planning, identifying victims/witnesses and other sources of information. These issues all continue to matter even after the investigation or documentation process is over, because the team still has an obligation to maintain the security and confidentiality of the evidence or information they have collected. This obligation may last for decades.

However, the trainer should emphasise that the participants cannot wait until the end of the process to start thinking about how to safely store and manage their information. From the planning and preparation phase and throughout the whole process, they need to think carefully about the purpose of their investigation or documentation, what kind of information is necessary or appropriate for them to collect, the different forms that information might take (testimony, documents, physical material, digital or audio-visual, forensic), whether they have the relevant training or authority to collect that type of information, whether it will be practically feasible for them to document, collect or transport that information safely, and whether they can store the information securely and to the required standard over a long period of time. The trainer should make this point clearly at the beginning of Module 7/Part IV – Documentation in Practice: Preparation, and should emphasise it repeatedly throughout all subsequent modules. Planning and consideration of storage requirements is a vitally important issue and must happen from the very beginning of the investigation or documentation process, before the participants have collected any information or commenced any investigative or documentation activities. The trainer must ensure that they understand that it is too late to consider transportation, storage and maintenance after they have already collected the information.

For each of the types of information covered in this module – documentary and physical, digital and forensic – the trainer should ask the participants to consider how likely they are to be collecting that type of information, and whether their current facilities (such as office, computer or external hard drives, cloud storage) would have the physical space, digital space (memory) or other necessary resources to be able to store and protect it long-term. If they are already collecting and storing this kind of information, the trainer should encourage them to discuss (in general terms) what security measures they have in place to keep the information safe and confidential, what restrictions their organisation imposes on who can access the information and for what purpose, and whether they have ever encountered problems with personal or sensitive information which was not stored correctly or appropriately. All organisational decisions regarding these matters should be documented in a policy document that can be later consulted and updated if necessary, and which could later be provided to judicial officials who may need to understand the data handling and storage procedures in order to use the information as evidence.

Depending on the background and experience of the participants, the answers might range from a bicycle lock on a filing cabinet to a bolted evidence room, but the important thing to emphasise is that they are responsible for finding a way to make sure that the information continues to be protected. Regardless of the size and resources of their organisations, they need to be aware that without a specific plan for the storage and management of sensitive information, promises they have made and steps that they have taken in good faith to respect the principles of confidentiality, Do No Harm and informed consent when dealing with a victim or witness can be undermined or undone completely if, for example, one of their colleagues later releases or misuses that information or if the information is stolen or damaged. The trainer should also emphasise that the more sensitive the information (i.e. personal or identifying details, photos or recordings, information about security threats or protective measures), the greater the responsibility to keep it safe and confidential.

Practitioners can use a manual storage system, a digital storage system or a combination of both. After slides 5 and 6 dealing with storing and handling general principles, the trainer should highlight specific requirements to manually store documents or other physical items (slide 7) – hard copy case files, printed photographs of injuries or a memory key/card containing a video-recording of a crime scene – as well as minimum steps and considerations to ensure the security and integrity of information stored digitally (slides 8-10) - scans of documents, recordings, digital pictures. The trainer should encourage participants to consider and discuss the advantages and disadvantages of using a digital system, as opposed to a manual storage system. During the discussion about advantages of digital storage (uses less physical space, easier to search, analyse and generate reports from, easier to keep multiple copies in different places) and the possible use of electronic databases, the trainer could flag that these can be particularly helpful to identify patterns of violations, as covered in more details in Module 14 (Analysing Evidence and Information).

In relation to forensic and medico-legal information (slides 12-14), the trainer should refer back to Module 10 (Types of Evidence of Sexual Violence) and Module 12 (Collecting Additional Information) and underline that forensic medical examinations/collection of medico-legal evidence should only be done by trained professionals, ideally at the same time as the provision of medical care and by the same person. If the participants are not able to process or store forensic information safely and competently or if they do not need it to prove specific facts, they should not collect it. The trainer should establish whether there are any forensic requirements for establishing sexual violence in the relevant jurisdiction (i.e. need for physical or biological evidence/medical examination for a criminal trial, producing statements or medical certificates to be granted civilian victim status) and should ask the participants if they have any experience in collecting or preserving that kind of material, particularly over long periods of time.