Child PIP Data Management & Storage

The job isn't finished until the data is safely stored

General Principles

- Need to balance access to information with patient confidentiality
- Like other hospital records, Child PIP data is confidential. All staff who work with the data need to be made aware of this.
- The data remains the property of the facility.
- Each Child PIP site should have a written guideline regarding where records should be kept, and who should have access to them.
- There should be a designated person who takes responsibility for ensuring that the guidelines are followed. The provincial Child PIP co-ordinator should maintain a list of all facilities where Child PIP data is kept, and the designated person for each facility.
- The facility guideline on data management must include a process for handover of the responsibility should the designated person leave the facility.
- Facility-specific Child PIP data should ideally only be presented or published with the permission of the Clinical Manager or Hospital CEO.

Storage of hard copies

This includes monthly tally sheets, death registers and death data capture sheets, as well as minutes of mortality review meetings.

- The various forms should be well-organized, and kept in one designated place.
- They should be kept in a place which is only accessible to hospital staff.
- Death registers and death data capture sheets should be stored for a period of three years. After three years, the records should be destroyed (shredded).
- Minutes of mortality review meetings may be kept for longer, but processes must be in place to ensure that confidentiality of these records is maintained.
- Provision must be made for situations where a facility stops collecting Child PIP data. In this case the records should be placed in the care of an appropriate member of the hospital staff (this person in effect becomes the designated person for the facility, even though Child PIP is no longer being used). If this is not possible, the records should be given to the provincial Child PIP co-ordinator for safe-keeping. The data remains the property of the hospital.

Storage of electronic data

- Data should ideally be stored on a computer to which only a limited number of relevant people have access.
- An appropriate password should be used. This password should only be known by people who require regular access to the data.
- A backup copy of all electronic data should be stored on a different computer.
- Provision must be made for situations where a facility stops collecting Child PIP data. In this case the Child PIP data should be saved (on a CD or similar) and the information deleted from the computer – this is most important in situations where the computer to which many people have access is used. The CD can be stored with the hard copies (see above)
- Child PIP data should be readily available for analysis by all staff actively involved in the Child PIP process in the facility.
- Requests from other facility staff to use the information on the database should be dealt with on a case by case basis. In general, such users should not be given unlimited access to the database.