

Information security: a joint responsibility

The String of Pearls Initiative (PSI) collects clinical data and physical specimens from patients, for use in scientific research. This material has to be dealt with scrupulously at all times. Careful handling is vital to obtain accurate results and to gain the confidence of the people who provide their data and samples. It is also a legal requirement. To ensure the quality and security of the data, in 2008 the PSI board adopted a strict information security policy for the organisation.

The purpose of that policy is to bring all data management activities and flows of information within PSI up to the required standard and to maintain that situation. As such, it covers three key areas.

- Availability: access to the data;
- Integrity: the data's quality and clarity;
- Confidentiality: the use of pseudonymised data only, and solely for scientific research.

To achieve these policy objectives a set of measures covering technical, organisational and procedural matters is needed. Together, they form a balanced package which PSI expects the entire organisation to support and comply with.

Since the board considers information security an issue of vital importance, an Information Security Officer has been appointed and an Information Security Working Group established to guide and oversee practical implementation of the policy.

It is essential that all those involved with PSI, in whatever capacity, realise how crucial this subject is. They need to know what their responsibilities are and to be fully aware of the contribution they are expected to make. Information security has to be a "live" issue at all times, not merely a pile of papers.

Information security policy: key points

The working group has interpreted all relevant legislative and regulatory requirements, including Dutch standard NEN 7510 on information security¹, to cover

the situation at PSI. Three key points are at the heart of the resulting policy.

- Information security is the responsibility of the entire organisation, management included.
- Information security is a serious matter and so imposes strict standards upon all those who come into contact with PSI data, both within the core organisation and at its partner hospitals.
- Guaranteeing patient confidentiality is an absolute precondition for the provision of data.

The policy document outlines the measures required to ensure information security. They cover everything from overall policy to specific operational activities, including such topics as risk analyses of processes and data, staff training and guidelines, proper backup facilities, countering malicious software and good system access controls. The general descriptions are developed in greater detail in PSI's procedures and working instructions. For example, the policy is applied to the architecture and the design documentation of the various systems and processes used within the organisation. This ensures that careful handling of information becomes an integral part of everyday practice.

Scope

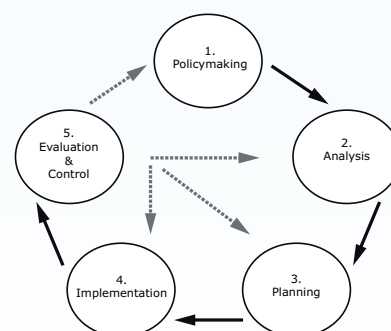
The information security policy applies to the entire PSI organisation. That is, both PSI itself and the associated departments at its partner hospitals. This requires thorough co-ordination with those institutions, the primary forum for which

is the established regular meetings of the joint Information Security Special Interest Group.

Information security and quality


Information security is a key aspect of PSI's overall quality assurance system. It therefore needs to be fully integrated into that system, with the policy measures it imposes incorporated in such a way that a high level of security is always maintained. To achieve this, and to ensure that the policy remains up to date at all times, a policy cycle has been introduced. This consists of five steps.

1. Establishment of the information security policy;
2. Analysis of the current situation, both centrally and locally, to understand the quality of the security measures now in place and the current risks;
3. Compilation of an information security plan and its adoption by the PSI board;
4. Implementation of additional security measures as required by the plan;
5. Regular checks that the desired effects are being achieved, with the cycle being repeated based upon the results.



Information security policy cycle

¹ this is the healthcare companion of the international ISO 27002 information security standard.



As with quality assurance, information security requires that the organisation complies with certain guidelines. To check that these are clear and that they have been anchored in day-to-day working practices, both internal and external audits will be performed at regular intervals.

The String of Pearls Initiative

The String of Pearls Initiative is the result of a unique partnership between the eight Dutch university medical centres (teaching hospitals). Founded in 2007 by NFU, the Dutch Federation of University Medical Centres, the initiative gathers clinical data and biomaterials from all the participating institutions so that together, they can promote the ad-

vancement of science, improve patient treatment and encourage the development of new products, as well as strengthening the economic position of biomedical research in the Netherlands. Initially, the project is focusing upon nine groups of medical conditions, its so-called "pearls". In the future, its activities may be expanded to include

others. For more information, you can contact the String of Pearls Initiative at info@string-of-pearls.org.