

## Accessibility to patients' data

### *Report 2005:1 Summary in English*

During 2004 and 2005 the Data Inspection Board carried out a project in order to investigate the processing of personal data within the medical service. One of the aims of the project was to look closer at the flow of personal data within the medical service and how case book data is shared between different divisions of the hospitals and between different care providers. It was of particular interest to look at how far the potential work with introducing coherent case books had got. The protection of personal data was checked, especially when the data was processed in wireless networks. The focus of the investigation was on hospitals.

During the period March-October, 2004, the Data Inspection Board investigated seven county councils and one municipality without a county council. In addition, the Board participated in network meetings and was in contact with representatives of Carelink, which is an interest association for county councils, regions, municipalities and individual care providers.

Developments within information technology in the medical service are accelerating and comprise many operators. New developing projects are constantly initiated. For a small authority like the Data Inspection Board it is difficult to oversee developments within all parts and be versed in everything that is going on. Therefore, the Data Inspection Board here presents some general points of view on what has appeared regarding supervision and pays special attention to the specific integrity risks that have been observed by the Board. The purpose of this report is partly to provide guidance when it comes to the considerations that have to be taken when new IT-systems are developed within the medical service and partly to constitute a basis for discussion.

It has been difficult to grasp the flow of personal data within the medical service since the county councils have chosen different solutions between themselves. Uniformity is lacking when it comes to the technology as well as the views on how accessible the patients' data should be. The case books of the hospitals are to a great extent still being kept on paper. However, a clear development tendency is that the patient's data gets accessible for more and more users over larger geographical areas as electronic case books are introduced.

Projects that aim at making patients' data more accessible are ongoing, on a regional as well as national level. For example, means have been distributed in order to develop a *national case book*. Experimental work with a *national patient survey* is already ongoing. At the same time the legal issues are under inspection.

The IT-systems are accessible to more and more users. However, working routines to check that unauthorized users do not get access to the data are still lacking to a great extent. The county councils usually expect that the routines will be improved on the long term. In practice this means that the county councils have very little, or no control, of who has got access to information about individual patients.

In certain county councils it is evident that an analysis of the flow of information in the organization has been done. After that, divisions that regularly co-operate are allowed access to one another's information. In other county councils it did not appear what considerations, if any, that had been made regarding principles concerning access to patients' data. With a permitting basis for access control, wishes to separate certain sensitive information from that

to which everyone has access often arise. The difficulty then is to decide which information should be accessible to everybody and which kind of information is too sensitive. The views on which kind of information that should be “blocked” in this way varies within as well as between the county councils. There are county councils that are of the opinion that all information regarding medical care should be processed in the same way and that no information should be blocked, while other county councils choose to limit the access to certain information.

As a summary, the following should be applied:

The guideline is that the patients’ data should not be made accessible to a greater extent than necessary.

An analysis has to be done regarding the need of information within the organization. It should be possible to vary the accessibility in regard to the need of information a certain official may have. The accessibility can be decided with the basis of for example position, medical speciality and established co-operation. Divisions that regularly co-operate because they belong to the same organization normally should be able to get access to one another’s information, assuming that the secrecy issues have been solved. There must also be efficient tools for follow-up and traceability. The identification of the user must comply with security restrictions.

There should be technical “thresholds”, which means that the user must make active choices in order to reach data about a certain patient.

There may be a possibility of a so-called emergency opening in emergency cases. If it appears that an emergency opening has to be used often, it may be necessary to change the principles regarding accessibility.

There should be tools to handle the requests of the patients.

There must be routines to handle secrecy marked personal data so that the risk of sharing such data with an unauthorized person is minimized.

The county councils need to improve their routines regarding follow-ups and check-ups of log files. A regular and systematic follow-up of log files is particularly important at a permitting basis for access control. In order to carry through meaningful analyses the county councils need to have technical tools.

The county councils need to have better control of the installation as well as the management of wireless networks. There should be a specific policy regarding wireless networks.