Information Security in Home Healthcare
Personal Integrity and Secrecy

(HS-IDA-MD-01-306)

Rose-Mharie Åhlfeldt
Department of Computer Science
Högskolan i Skövde, PO Box 408
SE-54128 Skövde, SWEDEN

Final year project
on the study programme in computer science 2001
Supervisor: Benkt Wangler
Information Security
in Home Healthcare
Personal Integrity and Secrecy

Rose-Mharie Ählfeldt

2001-10-08

I hereby certify that all material in this dissertation, which is not my own work has been identified and that no work is included for which a degree has already been conferred to me.

Rose-Mharie Ählfeldt
Abstract

Healthcare is very information-intensive. Hence, it has become necessary to use the support of computers in order to efficiently improve such an information-intensive organisation.

This thesis points out deficiencies in the area of information security in home healthcare regarding personal integrity and secrecy. Home healthcare is, in Sweden, performed by the municipalities. The work is based on the recommendations and common advice for processing of personal data compiled by the Data Inspection Board. Two municipalities in the Västra Götaland Region have been investigated. One of the municipalities has a manual system and the other has a computerized system for personal data management.

The work includes a field study where persons from both municipalities have been observed. It also includes interviews based on the comprehensive questions from the Data Inspection Board and questions arisen from the observations.

The work shows that a very clear need of training among personnel involved in home healthcare. It also shows the need for elaborate security measures including levels on access profiles. A weak point concerning security is also the heavy use of facsimile transmission for information distribution.

Keywords: information security, home healthcare, healthcare informatics, personal integrity, secrecy.
Acknowledgements

There are several people I would like to thank for their support during the work of this dissertation. First, I will give a special thank to my supervisor, Benkt Wangler, for his guidance and support. In addition, I thank the staff in the municipalities of Skövde and Mariestad for their participations. I also want to give a great thank to my close friend, Ruth-Marie Sörensson, for her valuable help and support with the English language. Finally, I would like to thank my beloved family, my husband Roland and my dear children Daniel and Emma, for their immovable support during the whole study programme in computer science.
Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>iii</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>iv</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Problem</td>
<td>1</td>
</tr>
<tr>
<td>1.1.1 Aim</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Research approach</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Expected result</td>
<td>5</td>
</tr>
<tr>
<td>1.4 Thesis outline</td>
<td>5</td>
</tr>
<tr>
<td>2 Background</td>
<td>6</td>
</tr>
<tr>
<td>2.1 Information systems security</td>
<td>6</td>
</tr>
<tr>
<td>2.1.1 Threats and risks</td>
<td>6</td>
</tr>
<tr>
<td>2.1.2 Reducing risks</td>
<td>11</td>
</tr>
<tr>
<td>2.2 Healthcare information systems</td>
<td>14</td>
</tr>
<tr>
<td>2.2.1 An overview of the information technology in the healthcare area</td>
<td>14</td>
</tr>
<tr>
<td>2.2.2 The acts that may cause an impact on the use of IT in healthcare</td>
<td>17</td>
</tr>
<tr>
<td>2.3 Home healthcare</td>
<td>21</td>
</tr>
<tr>
<td>2.3.1 What is home healthcare?</td>
<td>21</td>
</tr>
<tr>
<td>2.4 Information security in healthcare</td>
<td>22</td>
</tr>
<tr>
<td>3 Observations</td>
<td>28</td>
</tr>
<tr>
<td>3.1 The realisation of the observations</td>
<td>28</td>
</tr>
<tr>
<td>3.2 The municipality of Mariestad</td>
<td>28</td>
</tr>
<tr>
<td>3.2.1 Description of the home care unit in Marieholm</td>
<td>28</td>
</tr>
<tr>
<td>3.2.2 Summary report of the observations in Marieholm</td>
<td>29</td>
</tr>
<tr>
<td>3.3 Municipality of Skövde</td>
<td>31</td>
</tr>
<tr>
<td>3.3.1 Description of the home care unit in Timmersdala/Lerdala</td>
<td>31</td>
</tr>
<tr>
<td>3.3.2 Summarising report of the observations in Timmersdala/Lerdala</td>
<td>32</td>
</tr>
<tr>
<td>4 Interviews</td>
<td>36</td>
</tr>
<tr>
<td>4.1 Realisation of the interviews</td>
<td>36</td>
</tr>
<tr>
<td>4.2 Detailed questions</td>
<td>36</td>
</tr>
<tr>
<td>4.3 Summarising report of the interviews</td>
<td>40</td>
</tr>
<tr>
<td>5 Synthesis</td>
<td>46</td>
</tr>
<tr>
<td>5.1 Education</td>
<td>46</td>
</tr>
<tr>
<td>5.2 Levels on the access profiles</td>
<td>47</td>
</tr>
<tr>
<td>5.3 Facsimile as information distributor</td>
<td>48</td>
</tr>
<tr>
<td>5.4 Comparison between the manual and the computerised patient record system</td>
<td>49</td>
</tr>
<tr>
<td>6 Possible future research</td>
<td>51</td>
</tr>
<tr>
<td>6.1 Future research regarding education</td>
<td>51</td>
</tr>
<tr>
<td>6.2 Future research regarding access levels</td>
<td>51</td>
</tr>
<tr>
<td>7 Concluding remarks</td>
<td>53</td>
</tr>
<tr>
<td>References</td>
<td>54</td>
</tr>
<tr>
<td>Appendix</td>
<td>56</td>
</tr>
</tbody>
</table>
1 Introduction

Swedish healthcare has gone through an efficiency improvement the last few years but it will also encounter great challenges the next few years. Healthcare is a strongly information-intensive organisation and a great part of the business includes the exchange of information. Therefore it is natural to use the support of computers in order to efficiently improve such an information-intensive organisation.

With a new holistic view on the care offer and with a totally unbroken care chain from the emergency treatment and primary care to rehabilitation and home healthcare and home services of the municipalities, new ways of working and new technology solutions are required. It is not enough with only efficiency improvements of current procedures (Sågånger & Utbult, 1998).

Information security is defined as the collected effect of measures to minimise the risks addressed for the accessibility, secrecy, accuracy and traceability of information. If IT support is used for handling information the requirements are further confirmed. To perform proper information security there are some actions needed to reduce probability of service disruption, along with the prevention of unauthorised use (Lagerlund, 1999).

The increasing application of computers increases the accessibility of the data, especially when modern techniques, such as a network of terminals directly coupled to computers and local area networks are applied. Unauthorised use of the data is not an illusory danger. Therefore, the access to these data must be regulated. The fact that not everybody has access to the data is a logical consequence of the right to privacy. In addition, the individual must be able to check what has been registered about him or her and to whom data are distributed. Therefore, laws to protect privacy have been introduced and information security in the healthcare proceeds from laws, practices and ethics (van Bemmelen & Musen, 1997).

Healthcare is performed as care in hospitals, as primary care and as home healthcare. Healthcare is performed by county councils, municipalities and private care performers. The reform “Ädelreformen”, which came into force in the turn of the year 1991/1992, has transferred the home healthcare to the municipalities. The municipalities have gotten the liability for all care except medical efforts performed by physicians. The physicians are in the organisations of county councils or as private care performers. This implies that there is never a complete care team in home healthcare. Instead many organisations participate (Augustsson, 2001).

In this work the focus is on home healthcare.

1.1 Problem

The Data Inspection Board (DIB) has published a report about processing of personal data in hospitals. In this report they point out that the computerisation in the Swedish healthcare environment is widespread and further development in this area is expected.

---

1 Primary care – the first level of care comprising basic medical investigation, treatment and care.
Carefulness of the patient’s integrity and protecting the secrecy are a foundation view in healthcare. This view seems to be more important when data is computerised. In spite of this, the DIB considers defective management of patients’ data in the computerised area.

The DIB considers that The Act on Healthcare Records\(^2\) implies great freedom for people controlling personal data but also that the act puts demands upon these people. Mostly, the information to the patients must be improved. The controller of personal data\(^3\) must also meet a greater request in extracts from the records depending on the duty for controller of personal data to inform about the rights upon it.

The DIB establishes deficiencies in the Information Technology (IT) security regarding to patient data. Mainly, this depends on the nursing staff, which grasp the security measures as an extra pressure in an already hard working situation. Furthermore, the education in the security area has been neglected in many healthcare service units. Motivations for good security thinking seem also to be lacking (Datainspektionen, 1998).

The DIB gives recommendations regarding the basic security measures for the controller of personal data in the healthcare as follows.

- The nursing staff must always be vigilant that processing of sensitive personal data upon another national registration number does not happen. The patient’s identity must always be ensured through some form of checking.
- As the Act on Healthcare Records has come into force, every controller of personal data must, without delay, make strategies, which according to the Act, fulfils the strict demands of information.
- The controller of personal data must be certain that applicable constitutions or other rules are distributed within the organisation so the statutes can be followed.
- Workstations in use must never be left without control. It is impossible to act up to any form of IT-security if the workstations in use are left without control. Encroachment on patient record systems and other systems with sensitive data can easily be done with following unsuspected consequences.
- All users of the computer system should always use their own password and be sure that other users never use it.
- Screens with sensitive information should not be placed where passers-by have a direct view.
- Workstations accessible to Internet should be provided with virus-protection.
- The access-control manager must have checking routines so the staff no longer working in the organisation do not have access to the system.
- The controller of personal data must realise regular routines to check the IT-security in the organisation.
- All users in the computer system should be educated in IT-security continuously.
- Every acquisition of collection of personal data including sensitive information ought to be logged. The log should continuously be controlled.

\(^2\) The Act on Healthcare Records is a translation from the DIB for the Swedish word “Vårdsregisterlagen”.

\(^3\) The controller of personal data is a translation from the DIB for the Swedish word “personuppgiftsansvarig”.
The report from The DIB is dated from December 1998 when the Act on Healthcare Records just came into force. From the above, questions must be asked about how the current and future information systems in the healthcare meet the requirements of the Act on Healthcare Records regarding the recommendation from The DIB. The main focus of this work concern these questions.

To restrict this kind of work, some delimitation must be done, suitably by taking some unit in the healthcare in focus, e.g. home healthcare. Further description of home healthcare can be found in section 2.3.

- 1 January 1992 the “Ädelreformen” came into force. This reform implies that the municipality got a total liability for long-term services, nursing and care to elder and disabled citizens. The allotment of liability between municipalities and county councils changed. The municipalities got the responsibility of payment for efforts including long-term services and nursing to elderly and disabled citizens but still performed by county councils or single healthcare providers (Datanspekktionen, 2000:2).

- Since the “Ädelreformen” came into force, it is the primary municipalities in the Västra Götaland Region having the liabilities for both basic and advanced home healthcare. For both these parts some sort of a survey ought to be done to see how the systems managing personal data regarding patient’s integrity and secrecy protection meet the requirements performed by the recommendations of the DIB. Are there any lacks in the systems and what can be done to improve the systems?

- Today, the systems managing the personal data in home healthcare are usually manual but computerised systems exist even if they are in an initiating phase. In the case of manual system, what kinds of information are sufficient and necessary for the healthcare staff bringing into the working-place? In computerised systems, what is needed in the implemented systems, e.g. by hand-computers, to ensure the information security regarding the patient’s integrity and secrecy? In both these cases there is an interest to see how the systems meet the requirements from the recommendations of the DIB.

1.1.1 Aim

The aim of this work is to survey security problems concerning secrecy and personal integrity in systems managing personal data in home healthcare. The work is based on the recommendations and common advice for processing of personal data compiled by the DIB. Moreover, the aim is to establish how the existing and future systems can support the users in fulfilling the recommended security requirements.

More precisely, the objectives derived from the aim above are to find the answers of the following questions for both manual and computerised systems (cf. recommendations from DIB on page 3):

- How is the patient’s identity checked?
- What strategies exist to ensure that the strict information requirements enforcing by the act are adhered to?
• How are the constitutions and other organisational rules distributed to the staff so as to ensure that the proper statutes are followed?
• How is unauthorised access prevented in patient records? What are the needs to improve the protection against unauthorised access in existing and future systems?
• Are there any clearly distinguished levels of access? Are there any persons in charge keeping the authorities up-to-date?
• Are there any routines for following-up the information security in the organisation?
• Is there any existing educational programme in the organisation in order to educate the healthcare staff in information security policy?
• Is sensitive information in the system logged? How is the log checked and managed?

1.2 Research approach

To make a reasonable and complete survey, an empirical study should be done in the form of interviews with the responsible persons in home healthcare, and interviews with the healthcare staff working in the home healthcare. Furthermore, a field study could be a desirable activity performed to get a relevant idea of how the management of the personal data works by following the healthcare staff in their work in the home healthcare.

To accomplish the above, two municipalities in the Västra Götaland Region have been chosen. These municipalities are responsible for both basic and advanced home healthcare as is described in section 2.3. One of the municipalities has a manual system and the other has a computerised system for personal data management.

In the field study, continuously called observation, six persons have been chosen; three persons from each municipality. The observations have the following construction; the observer follows the observed professional during the day of working and notifies in a notebook interesting events and routines. The observations will be occurred unprejudiced and described in a form of diary where the routines are as clearly described as possible.

After the observations, the notes will be rewritten and then the observed people have the opportunity to read through the text. The aim is not to give the observed people the opportunity to change something. Observed things are observed. Instead, the aim is to inform the observed people what has appeared and that there are no misunderstandings.

The base of the work with the interviews will be the comprehensive questions from the objectives, but also questions arisen from the work with the observations. The interviewed persons can be district nurses, staff nurses and nurse’s aides. These persons will also take part in the observations. Furthermore, two unit managers and two MAS\(^4\) will also be interviewed. In total it will be ten persons who take part in the interviews, five from each municipality.

The interviews are intended to occur in a discussion form together with the persons concerned at their workplaces. The interviewed persons will not see the questions before

\(^4\) MAS – a Swedish acronym for medical responsible nurse, in Swedish: medicinsk ansvarig sjuksköterska
the interviews. The interviewer asks the questions and the interviewed persons will answer to best of their ability and then the interviewer notifies the answers. The answers will be rewritten and then sent to the interviewed persons for validation.

1.3 Expected result

More than two years have gone since the acts came into force. Moreover, more than two years have gone since the DIB issued the report of personal registrations. In spite of all this, there are still deficiencies in information security regarding personal data and patient’s integrity in existing computerised systems managing information in home healthcare. Furthermore, one can expect that the manual system is more defective than the computerised system depending on basic limitation in manual systems. The reasons to the defectives can depend on the staff still being hard pressed in a working situation under stress, but also that compiled action programmes of connections between acts/strategies and practical realisation are missing or unclear.

In addition, an expected result could also be to see if there are any possibilities to improve the existing information systems in the home healthcare regarding to information security. Furthermore, to see how future information systems can be developed so they can give a better support for the information requirements enforced by the Act on Healthcare Records and the Personal Data Act, and perform the recommendations from the DIB. This result may be foundation material for future research in this area.

1.4 Thesis outline

The rest of the thesis comprises:
Section 2, which provides an extended background concerning general security problems in information systems, an overview of the information technology in the healthcare area, a brief description of the home healthcare area, and information security in healthcare.

Sections 3 and 4, provide the results from the observation and the interviews respectively.

In section 5, the work is analysed and the important main points are described as a result from the work.

Section 6, provides the possible future work from the main points from section 5 and the last section provides a connection to the aim of the work.

At the end of the thesis, there is an appendix including the glossary of terms and abbreviations used in the work.
2 Background

2.1 Information systems security

Information system security is an extensive area and to give a basic description of the whole area of the information system security problem is out of the scope of this work. Nevertheless, it is important for the work to give a brief description of the basic security problems in computerised information systems.

2.1.1 Threats and risks

This section gives a brief description about the main threats and risks in the information systems area. The section is divided into three parts. First, threat of accidents and malfunctions are described. The second part describes the threat of computer crime and finally factors that may increase the risks are described. If nothing else is mentioned, the main material content is referred to Alter (1999).

**Threat of accidents and malfunctions**

Many people assume that information systems will work as they are designed to work, that they will operate reliably, and that the information generated will be correct. When these assumptions are proven wrong, the consequences can be disastrous.

The accidents and malfunctions can be divided into five points.

- Operator Error
- Software bugs
- Data errors
- Damage to physical facilities
- Liability for system failure

**Operator Error**

A prime cause of accidents is operator error, a combination of inattention, non-conformance to procedures, or other error by participants in a system.

A careful study of accidents in complex systems such as nuclear plants, dams, tankers, and aeroplanes found that 60% to 80% of major accidents were attributed to operator error, but that many factors other than operator carelessness contributed to the problems. These factors included flawed system design, poor training, and poor quality control.

The main point is that all systems are vulnerable to human error.

Although significant hardware malfunctions are becoming more and more infrequent as computer technology improves, these problems do occur occasionally. Vulnerability to hardware malfunctions is often magnified by user disbelief that hardware can malfunction. Furthermore, as software functions are integrated into hardware, what is seen as hardware can have bugs just like software?
Software bugs
A software bug is a flaw in a program that causes it to produce incorrect or inappropriate results. Isolated software bugs have caused significant financial loses even in large, well-run organisations.

Software bugs are a fundamental problem with computerised systems because there are no infallible methods for proving that a program operates correctly. The best-tested software may still have bugs after testing is complete. Even if it were possible to prove that a program operates correctly relative to its design specs, there is no guarantee that it will operate correctly under unanticipated circumstances.

Data errors
Information systems in everyday life frequently contain errors such as incorrect phone numbers or addresses. Many errors due to carelessness and inattention therefore cannot be detected automatically.

Damage to physical facilities
Physical facilities and equipment may be vulnerable to a wide range of environmental threats and external events. In the last few years, fires, floods, hurricanes and earthquakes have damaged computer facilities. Computer and telecommunications equipment may be disabled to power failures and network breakdowns occurring far from the site. Damage to physical facilities doesn’t require a natural catastrophe. Events miles from their facilities may affect individuals and businesses. Firms relying on information systems need to protect their own facilities and need to prepare for impacts of problems elsewhere.

Liability for system failure
Liability is legal responsibility for one’s actions or products. Every type of accident mentioned above can result in a liability claim against a firm or individual. This is an especially serious potential problem in medical systems. Liability is also an issue in business software. Liability related to information systems is complex because so many different things can go wrong. Given the potential for product liability lawsuits, software vendors are usually careful to avoid claiming their software is bug free. Their license agreements usually state that any problems resulting from the use of the software are the user’s fault.

Threat of computer crime
Computer crime is the use of computerised systems to perform illegal acts. It can be divided into two main areas: theft, and sabotage and vandalism. Computer pranks are included as illegal activities because they often have at least the potential for significant harm. Also they may be difficult to differentiate from sabotage and other forms of destructive behaviour.

Computer crime is growing more worrisome as computerised systems become more pervasive. The potential for significant damage to commercial interests and national defence through computer viruses and other forms of computerised sabotage has been demonstrated clearly. Weaknesses exploited often involve technical gaps between what a computer system is capable of enforcing and what it is expected to enforce. Other
weaknesses involve gaps between computer policies, social policies and human
behaviour.

Most computer crimes go undetected and those that are detected often go unreported.
But by any estimate, computer crime costs billions of dollars every year (Beekman et al.,
1997).

There is no single profile for computer criminals. They range from application
programmers and clerical personnel to managers and accountants. In general,
perpetrators of computer crime can be divided into employees, outsiders and hackers.

Employees use their knowledge of how a business operates to identify opportunities for
theft or sabotage and to obtain easy access to the resources they need for their criminal
activity.

The typical computer criminal is a trusted employee with personal or financial problems
and knowledge of the computer system. The most common computer crime, software
piracy, is committed by millions of people often unknowingly (Beekman et al., 1997).

Outsiders often have a somewhat more difficult task because they must learn how to
penetrate a system without having easy access to information about how it works.

Hackers are less concerned about personal gains or damage they might cause. Instead,
they commit computer crime for the “fun” or intellectual challenge of breaking into a
computer.

Theft

Theft is the most common form of computer crime. Computers are used to steal money,
goods, information and computer resources. All of these crimes are expensive – for
business, law enforcement agencies, and taxpayers and consumers who ultimately must
pay the bills (Beekman et al., 1997).

Computer-related theft can be divided into five categories: theft of software and
computer equipment, unauthorised use of access codes and financial passwords, theft by
entering fraudulent transaction data, theft by modifying software, and theft by stealing or
modify data.

- **Theft of software and computer equipment** has become a major problem for hardware
  and software manufactures and for companies that use computer equipment. Part of
  the temptation is that software, chips and computer equipment are both small and
  valuable. Theft of computers also causes problems because of the value of data on the
  computers.

- **Unauthorised use of access codes and financial passwords**
  Telephone credit card numbers, access codes, passwords and regular credit card
  numbers have all become major targets of criminals.

- **Theft by entering fraudulent transaction data**
  This is the simplest and most common method of theft in computer-related crime.
  Examples – forgery, impersonation fraud, disbursements fraud, inventory fraud,
  payroll fraud, pension fraud, cashier fraud.
• Theft by stealing or modifying data
  One way to steal data is by removing physical media such as paper documents, tapes, or diskettes. There are many stories of salespeople taking a customer list on leaving a job. The pervasive use of personal computers and diskettes makes this easy to do.

• Theft by modifying software
  Some programmers have committed computer crime by modifying software so it performs differently when it encounters a particular account number or other triggering condition.

Sabotage and Vandalism
Perpetrators of sabotage and vandalism try to invade or damage system hardware, software, or data. They may range from hackers to disgruntled employees to spies. The Internet has created many new possibilities for sabotage and vandalism and disgruntled employees who understand a computer system’s operation and its weak points are especially dangerous perpetrators of computer crimes. Disgruntled employees have erased, modified, and even kidnapped data and programs.

The names given to the saboteurs’ destructive programs, viruses, worms and ‘Trojan horses etc – sound more like biology than technology and many of the programs even mimic the behaviour of living organisms (Beekman et al., 1997).

A number of programming techniques have been used for sabotage and vandalism:
• A **trap door** is a set of instructions that permits a user to bypass the computer system’s standard security measures. Trap doors are frequently put into programs by programmers to make it easier for them to modify the software.

• A **Trojan horse** is a program that appears to be valid and useful but contains hidden instructions that can cause damage. For example, a Trojan horse could identify a particular account number and bypass it or could accumulate differences due to rounding and place them in a particular account. Trojan horse software hides an enemy in an attractive package. Trojan horse programs are often posted on public domain bulletin boards with names that make them sound like games or utilities. Trojan horses can cause serious problems in computer systems of all sizes. To make matter worse, many Trojan horses carry software viruses (Beekman et al., 1997).

• A **logic bomb** is a type of Trojan horse whose destructive actions are set to occur when a particular condition occurs, such as reaching a particular clock time or the initiation of a particular program. If the logic bomb is triggered by a time-related event, it is called a time bomb. Logic bombs are sometimes used for computerised vandalism and revenge.

• A **virus** is a special type of Trojan horse that can replicate itself and spread, much like a biological virus. A virus attached to a program is loaded into the computer’s memory when the program is loaded. The virus is programmed to find and insert a copy of itself into program or files that do not contain it. When those programs are executed, the copy of the virus starts up and attempts to replicate the virus again. Another type of virus is macro virus, which infects documents and can be transmitted via e-mail. Viruses are introduced into company computer systems in many different ways. Macro viruses are a common and serious threat because they can be transmitted accidentally if attached unknowingly to legitimate documents and e-mail. This is one
of the reasons it is important to use a virus scanner on incoming documents before opening them.

- **Worms** use computer hosts to reproduce themselves. But unlike viruses, worm programs travel independently over computer networks, seeking out uninfected workstations to occupy. A typical worm segment resides in a workstations memory rather than on disk so shutting down all of the workstations on the network can eliminate the worms. The popular press usually doesn’t distinguish among Trojan horses, viruses, and worms; they’re all called computer viruses (Beekman et al., 1997).

**Factors that amplifies the risks**

There are three major factors that increase the risks in information systems security area.

- The nature of complex systems
- Human limitations
- Pressures in the business environment

**The nature of complex systems**

Many complex systems rely on many different human, physical, and technical factors that all have to operate correctly to avoid catastrophic system failures. In addition to relying on everything to work correctly, computerised systems are often designed to hide things users don’t want to be involved in, such as the details of data processing. Although usually effective, this approach makes it less likely that users will notice problems. In addition, users often try to bypass computerised systems by inventing new procedures that are convenient but that may contradict the systems original design concepts. The more flexible a system is, the more likely that it will be used in ways never imagined by its designers.

Information system decentralisation and multivendor connectivity also affect security. As networked workstations become more common, the ability to access, copy and change computerised data expands. Electronically stored data in offices are highly vulnerable because many offices are low-security or non-security environments where people can easily access and copy local data and data extracted from corporate databases. Storage media such as diskettes, and even the computers themselves, are easy to move. Data channels such as electronic message systems and bulletin boards may be poorly controlled. These areas of vulnerability all result from the worthwhile goal of making information and messages available and readily usable.

**Human limitations**

Many users of office systems are unsophisticated about system security and ignore it. Other human limitations increasing system vulnerability include complacency, carelessness, greed, and limited ability to understand complex systems. Complacency and carelessness lead users and managers to assume systems work correctly and to lax enforcement of security systems. Controls, designed to prevent disasters in computerised systems, are often ignored by the people who are supposed to enforce them.

Greed and other human frailties increase vulnerability because they provide a motive for computer crime. People having personal problems related to drinking, drugs, gambling,
or other difficulties may see computer crime as a way to solve their problems. People who want revenge on their employer or supervisor may also resort to computer crime.

**Pressures in the business environment**
The business environment increases vulnerability by adding pressures to complete systems rapidly with limited staff. Information system vulnerability may not be considered adequately when development decisions are driven by needs to maximise return on investment. In the rush to meet deadlines with insufficient resources, features, and testing that reduce vulnerability may be left out.

The competitive environment has even pushed companies to reduce their executive level attention to security. Despite the argument that having a high-level security expert is more important to many organisations today than it ever was in the past, a number of high-profile businesses have shifted these responsibilities to their end-user departments.

### 2.1.2 Reducing risks
There are a number of methods for reducing risks in the information security area according to Alter (1999):
- Build the system correctly in the first place
- Train users about security issues
- Once the system is in operation, maintain physical security
- Given that it is physically secure, prevent unauthorised access to computers, networks, and data
- Having controlled access, make sure transactions are performed correctly.
- Even with transaction controls in place, motivate efficient and effective operation and find ways to improve.
- Even if the system seems secure, audit it to identify problems
- Even with continuing vigilance, prepare for disasters.

None of these methods are foolproof because many problems cannot be foreseen. However, consistent and thorough attention to the security and control value chain reduces the likelihood of accidents, computer crime, and ineffective usage.

**Controlling system development and modifications**
Software quality control is the process of assuring that software is developed efficiently, debugged completely, and maintained carefully and efficiently. Software quality control usually implies careful adherence to a structured system life cycle, regardless of whether the software was built in-house or by a vendor.

Maintaining software quality also calls for careful testing of any vendor-supplied software before it is distributed in the organisation. Although this may seem unnecessary because the software and computers should work properly, we have already seen many systems that did not work as intended. Problems and vulnerabilities of many systems are linked directly to bugs and design flaws that can be found through testing.

**Providing security training**
Complacency, carelessness, and lack of awareness all increase the likelihood of accidents and computer crime. Companies should train users to be aware of security concerns and
to understand how these concerns are related to rules and procedures. Every employee who uses a computer, or is at all involved with transaction processing, should be familiar with the major issues in information systems security area. They should also know some of the signs of suspicious activity and the company’s procedures for reporting that activity. Large losses are not surprising when employees are unaware of the risks or know that company management doesn’t care.

Maintaining physical security
Maintaining physical security is essential for protecting computing and communication facilities. Physical security measures should take into account threats including accidents, uncontrollable external events, and attack by intruders. Physical security starts with simple measures such as forbidding eating, drinking, and smoking near computer equipment. Just dropping a cup of coffee can damage equipment and erase data.

Physical access controls guard against physical access to computer facilities and data. The general guideline is to keep unauthorised people out of computer rooms, communication centres, and data storage locations.

Controlling access to data, computers and networks
Security measures should restrict access to confidential information and enforce mandatory ground rules.

Control technique
- Enforce manual data handling guidelines
  - Lock desks
  - Shared discarded documents and manuals
- Define access privileges
  - Give different individuals different levels of privilege for using the computer
- Enforce access privileges
  - What you know
    - Password
    - Special personal data
  - What you have
    - ID-card
    - Key to physical data
  - Where you are
    - Call-back system
  - Who you are
    - Fingerprint or handprint
    - Retina pattern
    - Voice pattern
- Control incoming data from networks and other media
  - Use firewalls
  - Scan for viruses
- Make data meaningless to anyone lacking authorisation
  - Data encryption
Controlling transaction processing
Control of transaction processing starts with data collection and includes the way computers process the data and the way errors are corrected. The control points include:

- **Data preparation and authorisation**
  Data preparation and authorisation create the transaction data that will be entered into a transaction processing system.

- **Data validation**
  Data validation refers to checking transaction data for any errors or omissions that can be detected by looking at the data. Common computerised validation procedures include checking for missing data (such as a missing social security number), invalid data (such as an impossible ZIP code), and inconsistent data.

- **Error correction**
  Error correction is an essential component of any transaction processing system because it is impossible to assure correctness of all data in the system, regardless of how carefully the data were validated when first entered.

- **Back-up and recovery**
  To make sure that whenever the computer system goes down regular processing will resume with minimal pain and inconvenience.

Motivating efficient and effective operation
Another side of system management is creating incentives for efficient and effective operation, especially monitoring information system usage and by using chargeback to motivate efficiency.

- **Monitoring information system usage**
  Well-designed information systems contain measures of performance both for the business process being supported and for the information system itself. Regardless whether the monitoring concerns business process performance, information system performance, or unusual activity, it has little value unless users and managers are willing and able to use the information.

- **Charging users to encourage efficiency**
  The lack of publicised measures for many computerised systems leads users to ignore their costs, use them inefficiently, and sometimes tolerate misuse. Chargeback systems try to motivate efficient usage by assigning to user departments the costs of information system. Impacts of chargeback systems on behaviour are apparent in the way offices operate. Even if resources aren’t free, the way they are charged out affects how they are used. Chargeback schemas should motivate people to use resources efficiently by reflecting the organisations true costs. The key issue in charging for using information system resources is to affect people’s decisions.

Auditing the information system
Auditing standard and controls are designed to ensure that financial operations are neither misrepresented nor threatened due to defective procedures or accounting systems. With the advent of computer systems, the scope of auditing expanded to encompass both general controls over computer installations and application controls for assuring that the recording, processing and reporting of data are performed properly.
Preparing for disasters
A disaster plan is a plan of action to recover from occurrences that shut down or harm major information systems. The need for such a plan is apparent from the potential impact of accidents, sabotage and natural events such as floods and earthquakes. The nature of extent of an information system’s disaster plan for a business depends on the role of information systems to the day-to-day operation of the business. The plans ought to be documented, distributed and tested.

2.2 Healthcare information systems

2.2.1 An overview of the information technology in the healthcare area
The Swedish healthcare has gone through an efficiency improvement the last few years but is also brought up against great challenges the next few years. Healthcare is a strongly information-intensive organisation and a great part of the business includes the exchange of information. Therefore it is natural to use the support of computers in order to efficiently improve such an information-intensive organisation.

Healthcare informatics can be expressed as medical informatics or nursing informatics depending on the functional area. Wainwright (1994, pp 180) defines nursing informatics as “the usual kind of definition of nursing informatics is the combination of computer science, information science and nursing science designed to assist in the management and processing of nursing data, information and knowledge to support the practice of nursing and delivery of care”. Petersson & Rydmark (1996) define medical informatics as the knowledge area comprising (1) data processing and communication in the healthcare business, (2) education and research, including information science and (3) technology to support their tasks. In this thesis, the term healthcare informatics is used and is defined as the combination of computer science, information science and medical science designed to support the practice of healthcare area, cf. Figure 1.

![Healthcare informatics](image)

Figure 1. Healthcare informatics

In spite of the fact that information technology (IT) has had a powerful penetration in society at whole, healthcare has been late in its establishing of IT in the business regarding to healthcare informatics. This depends, to the greatest part, on the complexity
that exists within healthcare. On the other hand, IT has been used for economy and administration. Because healthcare is an expensive expense for today’s society, it is in the interest of everybody to find efficiency improvements, which implicates timesaving and efficiency in all areas. IT will give rise to radical effects within healthcare, medical education, and research (Petersson & Rydmark, 1996).

With a new holistic view on the care offer and with a totally unbroken care-chain from the emergency treatment and primary care to rehabilitation and home healthcare and home services of the municipalities, new ways of working and new technology solutions are required. It is not enough with only efficiency improvements of current ways of working. New technologies, in forms of tele-, computer- and other media-communication, can give opportunities to support a development of IT-support for the care process. New technology opportunities can be used to satisfy the need of information and knowledge to facilitate the decision process, treatment and planning concerning patients on both a general level concerning care-plans and guidelines for groups of patients and diseases, and on a patent specific level where patient specific data are included in the decision process. To decrease both time of care and waiting-time, and to increase the quality of the care, the information must be available for the care performers who need it, as quickly as possible, no matter where they are in the care-chain. One condition is that the information is current and correct, which is not always the case when the flood of information in the care stream is without computer support (Sågäng & Utbult, 1998).

The following-up of the business becomes better and the criteria of diagnoses and treatments get more unitary when the care staff takes the information technology, as a help, to collect, process, analyse and store statistics about how many patients are treated, what diagnoses they have, what medicines they use etc. The computer-stored and processed care information in record systems is also very useful for the research which gradually gives the patients advantages in form of totally new and better methods of making diagnoses and treatments. Excellent information systems contribute to create a general view in different kinds of business about expense and facilitate analyses about how efficient the business is (Sågäng & Utbult, 1998).

*The patient record*

One of the most central units in care information is the patient record. The traditional paper-based patient record used in a clinical setting generally contains the notes of clinicians and other care providers. These notes are often supplemented with data from other sources; laboratory test results and reports describing the results of other tests that have been performed, such as X-rays, pathology, ultrasound, lung function and endoscopy (van Bemmel & Musen, 1997).

This type of records is generally defined as source-oriented. According to van Bemmel & Musen (1997), there are three different types of records. The time-oriented record has the notes in a chronological order. In the problem-oriented record each patient is assigned one or more problems. Notes are recorded per problem according to the SOAP-structure. SOAP stands for subjective (S), objective (O), assessment (A) and plan (P). The third type, the source-oriented, is both time-oriented and problem-oriented. The contents of the record are ordered according to the method by which they were obtained; notes of visits, X-ray report, blood tests, and other data become separate sections in the
patient record. Within each section, those data have a chronological order. Problem-oriented recording following SOAP, affects only the clinical notes. An important question is how well the current paper-based records are suited for its purpose. As one may rightfully expect, the patient record is used first and foremost to support patient care. However, developments in healthcare have made this task more complex, and there is also a greater demand for patient data for purposes other than patient care (van Bemmel & Musen, 1997).

Dahlin & Arnesjö (1996) declare that the overall purpose of the patient record is to facilitate and support that the patient will be given excellent and secure care. This purpose presumes that record data is reliable and available when needed in the care and understandable for the care performers.

According to Dahlin & Arnesjö (1996) the patient record ought to be:
- a continuously updated, easily used and an assured working instrument in the care
- a correct source of information (data security)
- a juridical tenable document (lawfulness)
- an instrument for methodological, qualitative and quantitative following-up and development in addition to economic and administrative planning in the business
- an instrument for education

Well-recognised ways of using the patient record referred to van Bemmel & Musen (1997) include the following:
- supporting patient care
- a legal report of medical actions
- supporting research
- educating clinicians
- healthcare management and services

A paper as a storage medium for patient data has the following disadvantages according to van Bemmel & Musen (1997).
- the record can be only at one place at a time. It may not be available or it may even be missing.
- the contents are in free text; hence they are variable in order, possibly illegible, possibly incomplete and possibly ambiguous.
- for scientific analysis, the contents need to be transcribed with potential errors.
- paper-based notes cannot give rise to active reminders, warnings, or advice.

The increasing demand for well-structured and accessible patient data, in combination with developments in computer science, sparked a great interest in the development of an electronic patient record. Computers have the potential to improve legibility, accessibility, and structure, but these pose heavy demands on data collection (van Bemmel & Musen, 1997).

Despite all of the developments regarding the computer-based patient record during the last few decades, it is still only used on a small scale in most settings. The strong focus on the shortcomings of the paper-based record has pushed its strong aspects to the
background. According to van Bemmel & Musen (1997), the paper-based record has five strong advantages and the computer-based patient record has seven principal strengths.

Advantages of paper records
- they can easily be carried around
- much freedom in reporting style
- easy data browsing
- requires no special training
- never ”down” as computers sometimes are

Advantages of computer-based patient record
- simultaneous access from multiple locations
- legibility
- variety of views on data
- support of structured data entry
- decision support
- support of other data analysis
- electronic data exchange and sharing care support

Developers have understood that it is not sufficient to eliminate the limitations of the paper record; its strengths must also come to expression in its electronic equivalent. An important problem of a logistic and financial nature involves data entry and display at the patient’s bedside. Beside computerised equipment is usually available only in intensive portable equipment, preferably with a wireless connection to the host system (van Bemmel & Musen, 1997).

2.2.2 The acts that may cause an impact on the use of IT in healthcare

The healthcare is controlled by a big number of acts, orders and statutes. Below, a brief description of the most important acts that cause an impact on the use of IT in healthcare is given.

**The Patient Record Act**

The Patient Record Act (SFS, 1985:562) came into force 1985 and is technically independent, i.e. it concerns information on paper or in any other form of medium. The act uses the term journal documentation, which implies everything pertaining to medical information. Those persons who are obligated to handle patient records by the act are on one hand; people with certification or specific appointment to engage in a special profession, and on the other hand; people who have no certification but perform working tasks which in other cases would be performed by speech therapists, psychologists or psychotherapists. In addition, people who work as occupational therapist, almoner or hospital physicist are also obligated to handle patient records by the act (Sjölenius, 1996).

The patient record shall be recorded in circumstances of care, examination and treatment of patients within healthcare. A patient record shall contain data about the patient’s identity, anamnesis, diagnosis and the treatment and requirements of care. Furthermore,
the record shall contain data regarding who made a note and when the note was written. The record note shall, if there is nothing particularly preventing it, be signed by the person who is responsible for the data (Sjölenius, 1996).

It is important for the credibility of the healthcare that security is guaranteed and that no record data is accessible to the attention of unauthorised persons. In this context, one can talk about internal and external secrecy. The patient record regulates the internal secrecy, i.e. questions concerning the routines for the using of the patient record within the business area where the patient record is stored. The external secrecy is regulated by The Secrecy Act (Sjölenius, 1996).

In the §7 it is prescribed that every handling of the patient record is to be handled and stored so no unauthorised persons can have access to it. In the case of care, it is just the limited part of the staff that needs access to the patient record in their work. The respect for the patient’s integrity requires that no one outside this circle has access to the record. Reading a patient record out of sheer curiosity can never be permitted.

Data in a record document may not be deleted or made unreadable in other cases than that which is referred to §17 in The Patient Record Act, and also in the cases of prescribed screening. When correction of faults and errors are concerned, it should be shown when the correction was done and who made the correction (Sjölenius, 1996).

If a record document, a transcription or a copy of the document has been distributed to someone else, it shall be signed in the patient record who has received the document, transcription or copy and when the record had been distributed. A record document shall be stored at least three years after the last data was recorded in the patient record (Sjölenius, 1996).

**The Secrecy Act**

The Secrecy Act (SF: S, 1980:100) is an act concerning regulations about the obligation to observe professional secrecy in public business and prohibiting the distribution of public documents. The afore-mentioned includes limitations of the regulations for the rights to access public documents provided in The Freedom of Press Act. The regulations concern the prohibitions to displaying information whether it is done orally, or by distributing public documents in another way. The Act also includes regulations concerning limitation on the right to leave messages for publishing or in radio programmes, films, audio recording or other mediums where basic regulations are given in The Freedom of Press Act and The Freedom of Speech Act (SF: S, 1980:100).

In the Act, the primary purpose of secrecy is to protect people’s privacy. In healthcare, secrecy applies for information about the state of health or other private circumstances of the individuals if it is not clear that the information can be revealed without any disadvantages for the private person or someone close to him. Furthermore, the secrecy applies in business regarding the management of medical records in private healthcare, information about the state of health or other private circumstances of the individual. Information can be given to the healthcare staff if it is necessary for the treatment of the patient. The secrecy for public documents is in force for at most seventy years (Sjölenius, 1996).
The Personal Data Act

The Data Act (SFS, 1973:289) came into force 1973 and was one of the first acts in the whole world concerning restriction in the treatment of data. The Data Act implied license requirements to store names or other computerised data about persons. The purpose of the act was to protect the person from indiscreet guarding and surveying by automatic data processing – by governments or other private interests (Carlén-Wendels, 1998).

Today, almost every storing of personal data is in digital form and exists almost everywhere e.g. in authorities, hospitals, banks, employers, associations, member records etc. The protection of the integrity has so far been succeeded fairly well depending on the isolations of the databases and records. Permissions to integrate records between governments have been a common task during the last few years. Everything under the parole – “the person who has nothing to hide….” (Carlén-Wendels, 1998).

It is a widely spread public apprehension that the Data Act has become antiquated and lost its anchorage in the public legal conscience. There is estimation that about 10 % of all registers have required license (Carlén-Wendels, 1998). The above requirements have enforced a new act to be brought. An act more concerning about personal data storing without any particular bureaucracy but implies more restrictions about what is permitted and what is not (Carlén-Wendels, 1998).

The Personal Data Act (SFS, 1998:204) contains provisions to protect people against their personal integrity being violated by the processing of personal data. The Act, which is adapted to the EU rules, entered into force on October 24, 1998.

Processing of personal data includes, for example, collection, recording, storage, adaptation or alteration, compilation or retrieval. The Act also applies to personal data that is transmitted, disseminated or made available by other means. There is no requirement that data, which is processed by computer, should be structured in a register or the like (Ministry of Justice, 1998).

There are some important exemptions from the Act. For example, the Act does not apply to such a processing of personal information as a natural person conducts for purely private purposes. This means that an individual may maintain an electronic diary or register of the addresses, etc. of his/her friends and relations. Word and text processing and communication with electronic mail also normally fall outside the ambit of the Act (Ministry of Justice, 1998).

Personal data may only be processed if the person who is registered (data subject) has given his/her consent to this. But here are exceptions. Personal data may be processed without consent when prescribed by statute. In some cases it may also be allowed if the processing is necessary in order that one may, for example, be able to make a contract with the data subject. Another case is, if it is necessary in order to comply with a legal obligation, or to protect a substantial interest of the data subject. Personal data may also be processed if necessary in order to perform a task connected to the exercise of official authority. Furthermore, in some special connections, the reasons for personal data being processed may outweigh the needs of the data subject to being protected against the violation of personal integrity. A data subject may revoke his/her consent. In that event.
Further personal data may not be processed. Very stringent rules apply to the processing of particularly sensitive personal data. Such sensitive personal data includes, for example, information about health, political opinion and religion (Ministry of Justice, 1998).

In the area of healthcare there exists a very extensive processing of personal data. Almost every unit in healthcare will soon be computerised. Computers and their information systems are used in cash processing, time reservations, examinations, at casualty department, clinics etc. These information systems have a character of sensitivity because the data in those systems concerns information of people’s health. Computerised medical records are common. The information in a medical record can be very sensitive. In a medical record the healthcare staff must notify everything needed for the care of the patient and then information may exist about compulsion care and criminality etc (Datinspektionen, 1998).

According to the report from DIB about personal registration in hospitals, the Data Act does not require any permission from the DIB in personal processing for authorities in the healthcare area. This exception concerns mostly patient administration systems according to hospitals and other care units (Datinspektionen, 1998).

According to computerised medical records there must exist permission from the DIB to manage those records because these records admit more information than health and illness, for example valuations, opinions, data about taken into custody, data of crime etc.

The Act on Healthcare Records


In The Act on Healthcare Record, the data, which is described as sensitive by the Personal Data Act, cannot be used as searchable terms in the healthcare record. On the other hand, the data regarding the ailment and patient state of health can be used. Only those who need access to the data in able to perform their work can have direct access to the data in the healthcare record. The acquisition of the data can only be referred to the data needed for the performance of the work (SFS, 1998:544).

The registered person may have access to information about the treatment of the record. According to SFS (1998:544), the information shall include among other things explanations about:
- who the controller of personal data is
- the purpose of the register
- what kind of information became an integral part of the register
- those regulations of secrecy and security which are enforced by the register
- the right to make corrections
- if the registration is voluntary
2.3 Home healthcare

2.3.1 What is home healthcare?
Home healthcare covers a big set of care in different forms, contents and organisations. Normally, the care is provided in the patient’s home and has some duration (Landstingsrevisorerna, 2000).

Home healthcare publicly is defined as non-institutional care that through the commitment and liability of the responsible authority is given in the patient’s home or wherever the patient lives. Generally in addition, the care should have some duration, usually more than two weeks even if shorter periods of care exist in practice (Landstingsrevisorerna, 2000).

Usually, the care is divided in basic home healthcare and advanced home healthcare depending on levels of care. Basic home healthcare includes levels 1 and 2, and advanced home healthcare level 3 (Landstingsrevisorerna, 2000).

- Level 1:
  Simple home healthcare, performed by district nurses and staff nurses. Co-operation of physicians is not required.

- Level 2:
  Regular home healthcare performed by district nurses, staff nurses and co-operation of physicians is required. Support from staff working in evenings or nights can be required but it is still basic home healthcare and managed by the family-doctor system.

- Level 3:
  Advanced healthcare in the home, requiring efforts throughout the twenty-four hours by a multi-professional team. This level is often described as “the hospital bed in the patient’s home”.

Home healthcare implies that health care is performed in the needed home. In reality, the business of home healthcare is more limited than that. Usually, the home healthcare concerns persons over the age of 18 who live in their own places and have a long duration of healthcare need. The majority of people nursed in home healthcare are elderly people (Socialstyrelsen, 1996).

The responsibility in the Swedish geriatric care has traditionally been divided into two responsible authorities. The county council had the total liability for measures that need medical competence, while the municipal had the liability for social efforts including living, social service, technical aid and economical support (Socialstyrelsen, 1996).

In the turn of the year 1991/1992, the “Ädelreformen” entered to force and gave the municipalities a collected liability for the old and handicapped citizens’ living and care except involving physicians. The municipalities got liability for nursing in specially livings i.e. houses of service, homes for the aged, group livings and nursing homes. The municipalities got responsibility of payment to the county councils for all somatic long-term medical treatment and for medically finished treatment. The responsibility of payment of the municipalities has probably contributed to shorter time of nursing at
hospitals for older patients and reductions of the number of beds in hospitals in the somatic short-term medical treatment. The goal for the care of old people in the future, emphasises the right to a living of one’s own, care attached to the area, needs for cooperation between different care-delivers, support from relatives and special forms of living and care for people in great need of help. Furthermore, the “Ådelreformen” has given the opportunities for the municipalities and county councils to make individual agreements about responsibility for organisation of primary healthcare and home healthcare. The organisations in nursing and care are because of that differing in the country (Socialstyrelsen, 1996).

2.4 Information security in healthcare

In this work the concept “information security” is used. It is a concept, which can be hard to give a definition, even for those people working within healthcare. Information in different forms is a necessity for the healthcare work and security is an obvious requirement for almost everyone anyone does in healthcare. Irrespective if it is a computerised or a non-computerised system that is handling the information in healthcare, the information demands should be the same. There are however some differences primarily that the use of computers in information handling allows access to stored information in a way not possible in non-computerised systems.

Some work has already been done in the area of information security. SITHS is a project with an aim to develop models and methods to realise the fundamental functions in information security in the support of IT in healthcare today and tomorrow. In their second report, the information requirements are summarised, without ogling at IT or other aids, as “Right information to the Right person in Right time and Right place”, cf. Figure 2 (Björner, 1999). This is more a vision than a definition they mean, and to further clarify the concepts, they will be described as follows:

- Right information implies that one is given correct and uncorrupted information to sufficient extent for the given situation.
- Right person implies that the given role in the given situation has access to the information. One person can be given different roles for different situations, e.g. citizens, politicians, physician etc.
- Right time implies that the information can be offered at the time it is needed.
- Right place implies that the information will be available where it is needed.

![Figure 2. Summary of the information requirements (From Björner, 1999, pp. 9)](image-url)
Information security is defined as the collected effect of measures to minimise the risks intended for the accessibility, secrecy, accuracy and traceability of information. Information security in healthcare proceeds from acts, practice and ethics.

If IT-support is used for handling information the requirements is further confirmed. To perform the vision about information security mentioned above, the SITHS-project has declared in the report (Björner, 1999) a summary of the basic functions as follows:

- **authentication**: checking the given identity
- **allocation** of authority; determination of the accessible rights
- **secrecy** and **confidentiality**: protection of information against improper observations
- **integrity**: protection of information against undesired changes, influences or observations
- **unrejectability**: protection against users or receivers of information having possibility to deny actions or knowledge about actions afterwards.
- Functions for **traceability**: possibilities to trace actions and events to a specific user and in this way keep proper users responsible for their actions.

The concepts above are clarified in Table 1

<table>
<thead>
<tr>
<th>Information security</th>
<th>Administration security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traceability</strong></td>
<td><strong>Integrity</strong></td>
</tr>
<tr>
<td>Distinctly derive performed operations to an individual.</td>
<td>Protection against undesired changes.</td>
</tr>
<tr>
<td><strong>Accessibility</strong></td>
<td><strong>Secrecy</strong></td>
</tr>
<tr>
<td>To use resources as required in expected extension and within desired time.</td>
<td>Data must not be accessible or unveiled to unauthorised people.</td>
</tr>
<tr>
<td><strong>IT-security</strong></td>
<td><strong>System security</strong></td>
</tr>
<tr>
<td><strong>Communication security</strong></td>
<td>Security that in main is obtained with help from related administered resources.</td>
</tr>
<tr>
<td><strong>Unrejectability</strong></td>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td>A reception or dispatch of a message can never be denied.</td>
<td>Check of given identity.</td>
</tr>
<tr>
<td><strong>Authority</strong></td>
<td><strong>Connect security</strong></td>
</tr>
<tr>
<td>The user’s right to use resources in the system</td>
<td>with transmission of information or steering signal</td>
</tr>
</tbody>
</table>

*Table 1. Information security (From Björner, 1999, pp. 46)*

All computer-stored information is vulnerable and specific measures must always be taken to secure data so care-providers can follow the acts concerning information handling in healthcare.

Dahlin & Arnesjö (1996) use data security as a security concept for computerised patient records. To say that a patient record has data security some issues are required as

- data does not get lost
- data can not fall into the wrong hands
- data is available when needed
- data is reliable

The issues above can be expressed in parts or protection shells, cf. Figure 3, which should be observed in quality judgement of data security of the computer record.
The protection shell **security** expresses identification/authentication, physical security, administration and construction.

The protection shell **authority** expresses rules and systems that guarantee that no unauthorised people can read, write or change data in the patient record systems. The patients must know for sure that the data they give is not accessible for others than those who need them. According to The Patient Record Act you cannot read a patient record if you do not need it for the care of the patient. The access is also a part of the legal security, which means that you are responsible for all you can do with support from the authority. In this sense, you cannot allow your access to be used by other care performers, not even for once. A password must also be chosen so it is impossible to guess it and it must also be kept secret (Dahlin & Arnesjö, 1996).

The protection shell **secrecy** expresses the access to stored data and is regulated by the acts concerning protection of the private individual. A more detailed description of the acts concerning the healthcare is given in the section 2.2.2.

The essence of the data security, **data integrity**, implies protection against undesired changes of the data.
The introduction of computers has increased people’s fear that their private life will be jeopardised. The individual must be able to check what has been registered about him or her and to whom data are distributed (van Bemmel & Musen, 1997).

An important element in the information security area is the awareness of the importance of data protection within the organisation. Activities are necessary to make the members of an organisation aware of the importance of data protection. This process will stimulate the recognition of the existence of risks on the one hand, and it will enhance the acceptance and the effects of measures to be taken on the other. This is a continuing activity in the organisation, since new staff will always be joining the organisation. There is also the danger that the attention to data security of those who have been in service for a longer time will relax over time (van Bemmel & Musen, 1997).

The access rights of users must be defined to protect data confidentiality. These access rights will depend on current legislation, public opinion, policies within the organisation, the attitude of professional organisations and so forth. Rules for data access depend, among other things, on the professional status of the user within the organisation, the patients concerned, the type of data, the relation between the user and the patient, the supplier of the data, and the age of the data. Access will also depend on the user’s intended action with the data, for example, read, write, edit, or delete (van Bemmel & Musen, 1997).

The SITHS project mentions two models to access information (Björner, 2000). They describe the authority model and the logging model, cf. Figure 4. The authority model implies that a user’s access to information is totally managed in advance by the regulated acquisition. The logging model implies that a user has full access to information on his/her own responsibility and all measures can be checked afterwards. The authority model has great demands on the person managing the authority, while the logging model mostly looks like other models legally applied in our society. Which model would be the best to chose? According to the SITHS project a combination is recommended. An isolated logging model runs the risk of minimising the trustworthiness for the information handling in healthcare, while an isolated authority model probably is overthrown because of the extensive administration this model is required.

Secrecy is another important element in the area of information security. The nursing staff has normally “to the backbone” that sensitive information must be protected against observation, against improper access and against manipulation possibility. At the same time there is an uncertainty among in the healthcare staff about the limits allowed in the performed information handling. This uncertainty has been strengthened by the introduction of IT in healthcare and by new legislation (The Act on Healthcare Record and The Personal Data Act), which has not yet gotten its fully interpretation and application. Even The Secrecy Act is partly hard to interpret, both its reach and its limitation to other legislation (Lagerlund, 1999).
The secrecy concept can be divided into internal and external secrecy. Internal secrecy implies that the person who fetches the information is responsible that the action is allowed, e.g. that the information is necessary as a basis to giving good care. The technology has given the opportunity to get the information directly accessible independent of the geographical distance. If this possibility, to get information from outside the own business unit is utilised, it implies that the internal secrecy business area has been expanded. Before the new technology possibilities came, the external secrecy dominated. The external secrecy implies distribution of information between independent business units, which in its most narrow interpretation has been the clinic. The sender is then responsible that the receiver has access to the information. The extension of the internal secrecy is support in The Act on Healthcare Record but has not an obvious support in The Secrecy Act (Lagerlund, 1999).

Healthcare is performed as care in hospitals, primary care and home healthcare. Healthcare is performed by county councils, municipalities and private care performers. The great variety of working forms is expected to increase. Business changes with bigger parts of division of labour are realised. This implies a greater co-operation between units within/or between organisations. The “Ädelreformen” has transferred the home healthcare to the municipalities. The municipalities have got the liability for all care except medical efforts performed by physicians. The physicians are in the organisations of county councils or as private care performers. This implies that there is never a complete care team in the home healthcare. Instead many organisations participate. This increases the complexity in information handling for the municipalities, which do not have long experience of healthcare liability. The municipalities have not kept up with the technical development and above all they have not created strategies and routines for the IT-security (Augustsson, 2001).
IT-support, as an integrated part of the healthcare process, makes new demands on the information systems as a whole. Co-operation implies community and agreements on many levels in the information handling and the IT-support. The open environment that follows with the increased co-operation, can increase the risks for unauthorised people to have access to the information or that the staff overstep their authorities. The own unit will be a part of one or many hospitals or be a part of the municipality home healthcare in teamwork with a number of private care performers (Lagerlund, 1999).

How do you then get a proper information security? In the third report the SITHS project declares that the most important element to get the information security to work in an optimal way is education (Björner, 2000). It is in the education existing threats, risks and possibilities can be pointed out. The SITHS group proclaims that this is the way to build security awareness. Measures of security, no matter how technically advanced they are, can never replace the knowledge of the staff and the attitude to the security work. Furthermore, it is enormously important that ethics and moral is kept on a high level. The healthcare process rests on an information flow where the security solutions are needed all the time (Björner, 2000).

To reach a good information security it is not enough with security functions and technology in the systems. Also, a structured way of working for the security work as a whole is required. The work must be impelled as a continuing process from the demands of the business to build up and maintain a conscious and adapted level of the information security (Lagerlund, 1999).
3 Observations

In this section, a conclusion of the work with the observations will be given. A more detailed description of the observations can be found in (Åhlfeldt, 2001a) where all observations are described in detail.

This section is divided into three parts. First, a description about how the observations have been realised, there after, one for each municipality, briefly describing the municipality and then a report, summarising the observations in the respectively municipalities.

3.1 The realisation of the observations

These municipalities that have been chosen in the Västra Götaland Region are the municipality of Mariestad with a non-computerised record system and the municipality of Skövde with a computerised record system called Magna Cura.

Six persons have been chosen for observation, three persons from each municipality. The observations have taken place during a period of two weeks and each observation had duration of one day. The observations have the following construction; the observer follows the observed during the day of working and notifies in a notebook interesting events and routines. The observations have occurred unprejudiced and are described in a form of diary where the routines have been described as clearly as possible.

After the observations, the notes have been rewritten and then the observed people had the opportunity to read through the text. The aim is not to give the observed people the opportunity to change something. Observed things are observed. Instead, the aim is to inform the observed people what has appeared and that there are no misunderstandings.

The municipalities do not use the term “patient” in their business of care. Instead, they used the word care-receiver. Continuously this word will be used in the reports of the observations and interviews.

3.2 The municipality of Mariestad

3.2.1 Description of the home care unit in Marieholm

In the municipality of Mariestad, the investigation object is the home care unit in Marieholm with a home for elderly called Myran. The unit has both a home for the aged where home healthcare is given, and also an external area where home healthcare is given for those living at home. The whole staff in the unit work both at Myran and in the external area, which they consider to be a varied and flexible system. There is one district nurse and 28 staff nurses and nurse’s aids in the area of Marieholm. The area has also one unit-manager, who manages the personal administration and investigates care-receiver’s allowance to home service. The district nurse has the MAS as superior medical manager. The district nurse allows home healthcare for care-receivers in the unit. In uncertain cases she will call for the MAS.
A description about the organisation of the care of old people in Mariestad is given in (Åhlfeldt, 2001a), in form of an organisation schedule for the care of old people of the municipality.

In Mariestad, the computerised patient records within home healthcare are in the construction phase. Education for the staff is in progress but yet they are in the initial phases. Therefore, the system they use today is still manual which implies that all patient records in Marieholm are paper-based and are placed in a locked metal-safe at the district nurse expedition. The archive of records is open during the day but the expedition door is not left unlocked. Out of day records are put in a special pile to be shredded by a document destroyer machine. Old records of care-receivers who have passed away or in another way been removed, are also collected in a stack for later delivering to the MAS.

Medicine lists from the pharmacy come in three copies, one is stored in the record, the second is stored in the file of care-receiver in the staff nurses’ expedition and the third copy is delivered to the care-receiver. Old medicine lists are stored in a special file in the district-nurse expedition.

The people, chosen for this work in the home-care-unit of Marieholm, are one staff-nurse, one nurse’s aid, and the district-nurse. These people have been observed for one day and also been interviewed. Furthermore, the unit-manager and the MAS have been interviewed. A detailed report of the interviews can be read in the report (Åhlfeldt, 2001b).

3.2.2 Summary report of the observations in Marieholm

In the following sections the observations of the district-nurse and the stuff nurses are summarised.

District-nurse

The district-nurse’s day begins with a report meeting together with the staff-nurses where up-to-date information from both district-nurse and the staff-nurses is exchanged. Then, there are a lot of phone-calls, partly from the care-receivers but partly the district-nurse herself making a lot of phone-calls. She uses the facsimile diligently. The care-receivers have many modifications in taking medicines, which generates new prescriptions and these are transmitted by the facsimile to the pharmacy. With the deliveries of medicines, new lists of medicines are included for respective care-receiver and are taken care of. The original is placed in the record, one copy to the care-receiver and one copy to the file of the care-receiver in the staff-nurse expedition.

The records are kept in the locked metal-safe. During the day it is open. Those care-receivers that have daily treatment are placed in the drawer and the records of immediate interest for the day are placed on the writing-table. The district-nurse works close to the records. During the phone calls she quickly puts up the record on the table and makes notes during the call. All data needed for other documentation comes from the record, i.e. writing admission notes, labels, orders etc.
The district-nurse has a computer beside her desk but she does not use it very much. She is connected to the municipality’s intranet and has access to the e-mail program and other applications. She checks the e-mail almost every day. Other than that, she does not use the computer very often.

During the coffee-break a new report is given between the staff nurses and the district-nurse about the current needs of care-receivers.

When the district-nurse does the home-visits she often puts the record in her bag. She does that, in case an emergency happens, she can quickly get the data from the record. She does not always note directly in the record while visiting the care-receivers, but it can happens.

Back at the expedition she finishes the writing in the records and puts them back into the drawer or the metal-safe. The information needed for the staff-nurses, she must write down in the files of the care-receiver herself. First, there is a front page and then a page of reporting. There is a lot of information written more than once, in part, in the care-receiver record in the district-nurse expedition and in part, in the pages of reporting in the files of care-receivers in the staff-nurse expedition. Even other files for different cards etc exist and must be managed. The cards and lists mentioned for the care-receivers are delivered by the staff-nurses the next time they visit the care-receiver.

Before the day is over, the district-nurse’s work includes sorting records and lists of medicine.

**Staff-nurses**

The staff-nurse and the nurse’s aid start their work with a run-through of the work for the day. The staff-nurse and the nurse’s aid are continuously called staff-nurses. They have a private agenda where they notify which care-receivers they are going to visit that day. They also check the files of care-receivers to see if there is something new about them. Above all, there is an oral communication between the staff-nurses, the district-nurses and the unit-manager at the reporting time. The files are on the table and they are not locked up when the staff leaves the expedition. On the other hand, they do not leave the expedition door unlocked. Other files or storage containing objects of value, i.e. file with patient-cards, box for the account card of the care-receivers, key-box with the care-receivers’ keys, are all locked up.

There is no identification-check when visiting homes. All care-receivers are well-known by the staff. When they get a new care-receiver, they identify the care-receiver by the name and address. The oral communication with the care-receiver determines if they are talking to the right person. When giving the care-receiver medicine they notify it on the care-receiver’s signing-list. They also notify wound-treatments on a specific list. Those lists are in the care-receivers’ departments and they are not in the record before the lists are full-signed. If there is something special, which must be notified in the record or the report page, the staff-nurses make a note in their own agenda so they do not forget it.

At coffee-time, once again, the members of the staff give reports about the care-receivers. There are many people on the staff, who feel pressure in their work. There are
wishes to give the work a better structure because there is a tendency that some working routines disappear depending on the unstructured work. A new system of working-times has been implemented and some people on the staff mean that this system does not give the right balance in the division of the work.

After coffee-time, if it is necessary, the staff-nurses do their documentation in the page of report or other lists. There are lists, including notes about which care-receivers have taken a shower, had their departments cleaned-up etc. These lists are not connected to the files of care-receivers; instead their purpose is a check for the staff so the care-receivers cannot proclaim that they have not received a service.

During discussions with the staff-nurses, where they think their work can be more automated by computers and perhaps laptop computers, which they can have for their own use in the field, they think this is an interesting thought because there is a lot of information, which should be important to have in the field. Moreover, there is an advantage to have a quick connection to other staff in the field. However, they are worried about replacing the oral communication between the staff with the computerisation because they do not want to miss this important form of communicating.

3.3 Municipality of Skövde

3.3.1 Description of the home care unit in Timmersdala/Lerdala

In the municipality of Skövde, the investigation object is the home care unit in Timmersdala/Lerdala. The unit has both a home for the aged, including five departments from which there are people suffering from dementia, and also an external area where home healthcare is given for those living at home. The staff is divided upon the home of the aged and the external area. The investigation area is the external area. There are one full time and one part time, 80 %, nurses and 18 staff nurses and nurse’s aids in the unit of Timmersdala/Lerdala. The area also has one unit-manager, who has personal administration-, environment- and budget-liability. There is also a home-care-secretary who manages application for investigations of home services etc. The nurses have the MAS as superior medical manager.

A description about the organisation of the care of old people in Skövde is given in (Åhlfeldt, 2001a), in a form of organisation schedule for the old people of municipality.

When the nurses work at weekends, they have the responsibility for the whole northern part of the municipality. The tasks are mostly scheduled but there are also tasks of emergency. Telephone and oral communication is the ordinary way of communicating between the employees.

The unit of Timmersdala/Lerdala has a computerised record system for one year. The aim is that all records will be computerised but there are still paper-based records. They have gotten directions from the MAS to make paper-copies from all records in the initiating phase. These copies are collected in files placed on the nurses’ desk. Today, they do not make paper-copies of all records. The other paper-based records are in a
lockable cupboard. The door to the nurses’ expedition is always locked when they are not in the room.

When they implement old records into the new system, they write a summary about the care-receiver’s history. They do not document everything from the old record into the new one.

The nurses’ authority implies access to the system and this includes access to records of all other units. This is an advantage for the pool-nurses and also for the staff working at weekends because the have got a large working area, not only one unit. Moreover, the nurses have access to other categories of records, e.g. physiotherapist, occupational therapist etc. The nurses can partly read the information, partly also make notes in the other record categories.

The system has also access to the registry of the national registration, which implies that the authority user has access to e.g. social numbers of all citizens in the municipality.

Those people, chosen for this work in the home-care-unit of Timmersdala/Lerdala, are one staff-nurse, one nurse and one district-nurse. These people have been observed for one day and also been interviewed. Furthermore, the unit-manager and the MAS have been interviewed. A detailed report of the interviews can be read in (Ahlfeldt, 2001b).

3.3.2 Summarising report of the observations in Timmersdala/Lerdala

In the following sections the observations of the nurses and the stuff-nurse are summarised.

Nurses

The district-nurse and the nurse, continuously called nurses, start their working day with a report time together with the staff-nurses about the work for the day. The staff-nurses go through the files of the care-receivers and discuss them one-by one to clarify each care-receiver’s special needs. If there is something new about the care-receiver it will be discussed. Then, the nurses continue the planning for the day in their own expedition. A common agenda is on the desk and in this agenda all planned home-visits of care-receivers are notified.

They start their computers and must log on to the intranet of the municipality before they can check the e-mail. Lately they have had some computer malfunctions. They were not able to switch off the computer in the right way but one of the nurses has received promises to get this problem fixed.

When they do home-visits they do not have any documents with them other than their own agenda on the trip. They do not write any notes during the visits. Instead the nurses try to keep new information in their mind.

At coffee-time, the nurses discuss the care-receivers with the staff-nurses once again and this time the question of secrecy is discussing. The care-receivers very often ask the staff
who the next care-receiver is. The members of the staff think it is hard to know how to behave in this situation because the care-receiver already knows who the next visitor is.

After the morning visits the nurses tick in their agenda what visits they have gone through. Also during lunchtime the nurses discuss with the staff-nurses about different concerns of the care-receivers that have appeared during the day. There are many telephone-calls, partly to KSS\(^5\) for consultations but there are also many calls to care-receivers. They do not get the personal data from the computerised records. They get the personal data from a file on the desk where copies of the computerised record are in paper-based form.

When the nurses are going to do their notes in the computerised records, one nurse gets the personal data from the file at the desk. She is not sure if it is possible to find the care-receiver by the name only.

Together with one of the nurses we examine the computerised record system. No notes can be made without an electronic signature. When the signature is accepted there is no possibility to change anything. If there is something wrong in the notes, the nurses must create an additional note to notify the changes. A home-visit without any comment, does not give rise to any note in the record.

The nurses have gotten instructions from the MAS to register the medicine lists in the care-receiver’s record. This has led to big problems, both for the work and also for the quality of information. The medicine lists come from the pharmacy once a week and can be of a large volume. These lists will then be registered in the record of the respective care-receiver without any control that the information is correct. The nurses proclaim that they do not trust that the medicine information in the computer is correct. Instead they look in the files where the original lists from the pharmacy are stored to make themselves sure about the right information. The registrations are also great demands for the nurses when they must take time for the registration instead of using it for the care. Electronical transformation of the lists of medicine from the pharmacy would facilitate the problem.

The system has also access to the register of national registration. When the care-receivers’ personal data are not complete, it can be an advantage to get the missing data from this register. There is a search-engine in the system but it is also possible to get a list with all names in the register and then find the desired name by scrolling in the list. When the nurses get the list a window is open and many names appear, approximately 15 names. In this list there are opportunities to have access to a lot of unnecessary personal data.

Presently, there are no connections between the system and the staff-nurses. The nurses make copies of desired information from the system and then put these copies into the files of care-receivers in the staff-nurse expedition. When the system is extended and the staff-nurses also have access to the system, there will be clear profit advantages.

\(^5\) KSS – a hospital in Skövde
The nurses mean that there are lacks in the education program of the system. One of the nurses has the document-responsibility for the system in the northern part of the municipality, which implies that she has gotten a concentrated course from the system developers. She has educated the rest of the nurses in the northern part of the municipality. The nurses are offered three days to get an education of the system. There is no specific education in security, instead the focus of the education is on the application and its functions.

There are deficiencies in the system and on one of the observation days there was a meeting when represented users together with the system-responsible person went through the deficiencies. They would discuss these deficiencies some days later at a user meeting together with the developers of the system. A list of the deficiencies from that meeting is described in (Åhlfeldt, 2001a).

**Staff-nurse**

The staff-nurse starts her work with a reporting time. One of the staff-nurses working on the evening the day before, goes through the files of care-receivers and takes care-receiver by care-receiver and discusses them together with the district-nurse about each care-receiver’s special needs. Those care-receivers with no changes are skipped over. The evening-staff always works the day after and are in charge of the reporting in the morning. After the reporting time they continue with the planning of the day. They notify in a special list which of the staff-nurses is going to visit which of the care-receivers.

All care-receivers that the staff-nurses visit are well known and therefore identification of the care-receivers is unnecessary. When a new care-receiver gets a home-visit, they identify the care-receiver most often by name, address and oral communication.

At coffee-time the staff-nurses communicate, partly to each other but also with the nurses about the care-receivers’ needs. The staff-nurse also makes notes in the file of care-receivers about which of the care-receivers whom have had a visit. Even if there is nothing of interest they still note in the reporting-page about the visits. Mostly to have an account that the staff-nurse has been at the care-receiver’s home, if the care-receiver would proclaim something else. The contents of the file of care-receiver consist of a reporting-page, a measure-page and common information about the care-receiver. Sometimes there are copies of the care-receiver’s records taken from the nurse expedition.

In a discussion with the staff about the need of information in the field, they proclaim that the staff is very well acquainted with the care-receivers so they do not need any more repetition of that information. On the other hand they proclaim the importance of oral communication. Notes in the files of care-receiver are very brief. Therefore, they need the oral communication.

The staff-nurses have a computer and they use it for making copies of lists and other forms. There is a large saving of time when using the computer for this task. The intranet of the municipality is used in order to get information and different kinds of news but also for electronic commerce of different stuff. There is a lot of information to get for the staff-nurses, but many of them cannot get this information because they do not have any
user name and therefore they do not have any access to the system. The system-manager has been notified that the staff-nurses at the unit should have a user name in common so they can get the information of the municipality.

When the staff-nurses do home-visits they sign a paper when the care-receiver has gotten some medicine. At such a visit, there was not any signature from the preceding staff-nurse. After checking with the proper person they signed it afterwards.

The day ends with a report meeting where the day-staff together with the nurses give the up to date information about the care-receivers to the evening-staff.
4 Interviews

In this section, a summary of the conducted interviews will be given. A more detailed description of the interviews and their results can be found in (Ahlffeldt, 2001b).

This section is divided into three parts. Firstly, there is a description on how the interviews have been realised. Secondly, there is a part showing the detailed questions from the comprehensive questions in the objectives. Thirdly, a brief description of the interviews in relation to the comprehensive questions is given.

4.1 Realisation of the interviews

The base of the work with the interviews has been the comprehensive questions from the objectives, but also questions arisen from the work with the observations. The interviewed persons are district nurses, staff nurses and nurse’s aid. These persons have also taken part in the observations. Furthermore, two unit managers and two MASs have also been interviewed. There have been ten persons in total who have taken part in the interviews, five from each municipality.

The interviews took place during two weeks, aside from one interview with a nurse who was ill at the moment for the interview and therefore was interviewed later. They have occurred in a discussion form together with the persons concerned at their workplaces. The interviewed persons had not seen the questions before the interviews. The interviewer had asked the questions and the interviewed persons have answered to the best of their abilities and then the interviewer has notified the answers. All interviews have lasted a little bit more than one hour. The answers have been rewritten and then sent to the interviewed persons for validation.

4.2 Detailed questions

Most questions are based on the recommendations given by DJB and their common advice in processing of personal data. The questions are modified depending on if the system is computerised or not. The questions are also adapted to the occupational groups of the persons. Some questions are from experiences and thoughts arisen from the observations of the persons referred to. A more detailed description about the observations can be found in (Ahlffeldt, 2001a).

Table 2 describes all detailed questions which are based on the objectives in section 1.3.2. The introductory questions give a brief description of the interviewed persons and the last questions are applied from the observations. An asterisk (*) has been used as a symbol of the occupational group of the person. Those questions, specifically aimed to a computerised system have a C after the asterisk and likewise questions specifically aimed to a manual system have an M after the asterisk. Other questions, with no C or M, have been asked to persons both in a manual and a computerised system.
Table 2. Interviewer questions

<table>
<thead>
<tr>
<th>Interviewer questions</th>
<th>Staff nurses</th>
<th>Nurses</th>
<th>Unit manager</th>
<th>MAS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introductory questions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For how long time have you had your position in the municipality and what does the position imply?</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>What is your experience, even private, of using computer?</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Which are the most common applications in your work? Do you store letters or other documents, including data about the care-receivers, in the server directly?</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>How is the checking of the patient’s identity managed?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How is the checking of a new care-receiver’s identity managed?</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Which are the basic principles of identifying care-receivers in the organisation?</td>
<td></td>
<td></td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Have you mixed up the care-receivers at any time, depending on having the same name, so they have got wrong care?</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td><strong>Which strategies exist to ensure that the strict information requirements enforced by the act are adhered to?</strong></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>According to the Personal Data Act and the Act on Healthcare Record, there are strict demands that the information to the care-receivers must be improved. Furthermore, the controller of the personal data must without delay make strategies such as the strict demands of information can be fulfilled as the act apply. Has the organisation, in your opinion, strategies to meet the requirements of information that the act demands.</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td><strong>How are the constitutions or other rules in the organisation distributed so the proper statutes are followed?</strong></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>How are the constitutions or other rules in the organisation distributed so you can realise them in the business? Are they sufficient in your opinion?</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>How are the constitutions or other rules in the organisation distributed so the proper statutes are followed? Is the information sufficient in the experience of the organisation?</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td><strong>How is unauthorised access prevented in patient records? What are the needs to improve the protection against unauthorised access in existing and future systems?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The own staff can make unauthorised access externally but also internally. The unauthorised access can be both intentional and unintentional. How is unauthorised access prevented in the manual respectively the computerised record system? Can the protection be improved? Should the protection be improved?</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Interviewer questions</td>
<td>Staff nurses</td>
<td>Nurses</td>
<td>Unit manager</td>
<td>MAS</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------</td>
<td>--------------</td>
<td>------</td>
</tr>
<tr>
<td>When the systems are connected to Internet or other open networks, the connection should be protected to prevent unauthorised traffic. For the same purpose, access should be prevented from the open network to another equipment or a local net at the liability of the personal data. If the data is given to identified users, the receiver should be ensured by encryption. Is the information in the system encrypted?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Are there clearly distinguished levels of access? Are there any persons in charge keeping authorisation up-to-date?</strong></td>
<td>*</td>
<td>*M</td>
<td>*C</td>
<td></td>
</tr>
<tr>
<td>To prevent unauthorised using or access, an access control system should be established. Also, in a manual system there are levels of access to data even if they can be harder to check. Yet, even a manual system must check the using, so only those who need the data for their work have access to the protected data. Are there any routines and principles in the organisation concerning what persons have access to the information in the record system? Are these principles clear? How does the organisation check that they are observed?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To prevent unauthorised using or access, a control-system of authorising should be established. Such a system should have the opportunities to identify the users and possibilities to confirm it, for example by using personal passwords. The system should have the ability to check the using so only those who need the information in their work should have the access to protected personal data. Also, there should exist routines for access control. What are your consideration about access and checking of authorities in existing systems? Are they clear and sufficient? Have you got any information about how often the authorities are updated, and what person in charge manages the updating?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Are there any routines for following-up the information security in the organisation?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you received any education in information security from the municipality? What knowledge have you got about the security policies of the municipality? Does the organisation follow-up and evaluate the policies? If yes, how often?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there any routine evaluation or following-up of the information security within the municipality? How often?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Is there any existing educational programme in the organisation in order to educate the healthcare staff in information security policy?</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there any existing educational programme to educate healthcare staff in information security in general? Is there any specific strategy for education in security questions when the computerised system is introduced?</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interviewer questions</td>
<td>Staff nurses</td>
<td>Nurses</td>
<td>Unit manager</td>
<td>MAS</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-------</td>
<td>--------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Is sensitive information in the system logged? How is the log checked and managed?</strong></td>
<td>*C</td>
<td>*C</td>
<td>*C</td>
<td></td>
</tr>
<tr>
<td>To check the access to the system, there should be, depending on the sensitivity of the personal data, a log file stored on a separate storage device. This log file should be followed-up and be protected against non-permitted changes. What is your knowledge about the log file in the system? Have you got any information about what data is stored in the log file?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Other questions applied from the observations</strong></td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What kind of information is the hardest to keep in mind when you are in the field?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What kind of information in your work is so important, in your opinion, that if it goes wrong, the consequences are negative both for the care and for the personal integrity of the care-receivers?</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are there any profits to have a mobile computer with you in the field, where all required information about the care-receiver is stored? E.g. what kind of care the care-receiver is entitled to, the latest directive from the nurses, and for your self to write down new information in the record necessary for the next working group?</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What kind of information, using in the daily work, is sufficient and necessary to bring to the care-receivers to get a qualitative care? Would a computerised system improve the opportunities to a more secure and better information processing?</td>
<td>*</td>
<td></td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>When a care-receiver passes away or in another way finishes the care process, the data must be archived for at least three years according to the Act of Patient Record. How is this data stored? Is it always available or is it stored in a separate storage device.</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One of the thoughts with the computerised system is to develop it further and then integrate the staff nurses to study the contents of the information stored in the system? How do you consider this development and what kind of information is most important for the staff nurses to have in the field, so they can give a qualitative and secure care? What are the requirements of the systems, in your opinion, partly in order to be a support for the staff nurses in their work, partly in the future, to give ensured protection for the care-receiver’s integrity and secrecy?</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medicine lists come today from the pharmacy in paper-based form. How will these lists be recorded in the future computerised system? Are there any plans to transform the lists into an electronic way?</td>
<td></td>
<td></td>
<td>*M</td>
<td></td>
</tr>
<tr>
<td>Today the medicine lists are recorded in the system in a manual way. The origins come from the pharmacy, and then they are recorded in a manual way in the computer, which can, for an inexperiance user, be a very busy task. Furthermore, there is no time to check that the data is recorded correctly. So, there is then an uncertainty of the quality of the information. Why this routine? Are there any plans to transform the lists into an electronic way?</td>
<td>*C</td>
<td>*C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.3 Summarising report of the interviews

In the following sections, a brief description of the results of the interviews is given. A more detailed description of the interviews can be found in (Åhlfeldt, 2001b).

Every main question from the objectives (cf. bullets on page 5) is described and concluded from the different persons that have been interviewed. If the questions are intended to both the manual and the computerised system, a description will be given for both systems in the respective question.

Introduction questions

All interviewed persons have long experience in their professions even if the present position is varied in time. In the respective municipality, the asked persons have worked from nine to thirty-two years.

In general, the asked persons only have a slight experience of computers. The nurses have experience of computers in their work but in private, they do not use the computer very often. The staff nurses, who do not have computers in their daily work, have very little experience about computers and they feel unfamiliar with the new technology, at the same time they are interested in the new technology and want to learn more about it.

Both of the unit managers, who have a nuanced job, work with a computerised application for the home services but they also use other applications such as MS Office, intranet of the municipality, e-mail etc. The unit manager in Timmersdala/Lerdsala also uses systems for personal administration, payroll and electronic invoicing. In Marieholm, the system for the home service is a part of the future computerised record system Procapita. This system also has a connection to MS Office where common letters and documents, including personal data, are written in Procapita to ensure the storing. The system for home services in Timmersdala/Lerdsala is quite old and does not have the connection to the computerised record system. Therefore common documents are stored in a disk of its own or at the server.

How is the checking of the patient’s identity managed?

The staff nurses almost never check the care-receivers’ identity by identity card. Instead, they nearly almost use the name or address and the oral communication to identify if it is the right care-receiver. Both Marieholm and Timmersdala/Lerdsala are small places and usually that the care-receiver is well known for the staff already at the first visit.
The nurses often use the name and address too to identify the care-receivers but it is more common that they check the care-receiver’s national registration number to ensure the identity. At the taking of specimens the national registration number is always checked. All respondents consider that there is no problem with the identification of the care-receivers. The computerised system does not give more support than the system has access to the register of the national registration of the municipality, which can be an asset if some data is missing.

The guidelines used by the municipalities to identify the care-receivers are in the quality- and security control of the department. Frequently, the staff gets the knowledge about the care-receiver by a care plan where data is already notified. The identification is considered more important when the care-receiver is moved to another care performer. The principle in both municipalities is that the nurse signs an identification-ribbon if the care-receiver is not able to take care of him-/herself, or if a relative or a member of the staff does not appear near by. In Marieholm they have changed the principle slightly and let the staff nurses also sign these identification-ribbons. The most important thing is how well known the care-receiver is for the person, who is signing, not in what occupational group the signing person belongs to.

Regarding the care-receivers with the same names the staff consider that it is a problem in the beginning but the staff must create special routines to manage that problem. Frequently, the name is modified either with additional symbols or with the place where the care-receiver lives. None of the asked persons has experienced that any care-receiver has got wrong care depending on name confusion.

**Which strategies exist to ensure that the strict information requirements enforced by the act are adhered to?**

There are no prepared strategies to meet the strict requirements enforced by the act, according to MAS in both municipalities. Today, information is given orally to the care-receivers but there are no written documents to distribute about the management of the records. The purpose is to prepare such documents, but it is not at the top of the priority list. None of the asked persons consider that the request from the registered persons have increased since the act came into force.

**How are the constitutions or other rules in the organisation distributed so the proper statues are followed?**

It is the MAS and the unit managers who have the liability to distribute the information to the staff.

In Marieholm, every two years the nurses get literature about up-to-date constitutions and other rules. Besides, the information is distributed by e-mail or in other paper-based form. It is common that the unit manager informs the staff at meetings but it is also possible for the staff to look in paper-based documents in the expedition.

In Timmersdala/Lerdala the most of the distribution appears by paper-based documents but it is the unit manager who is responsible and judges the extent of priority of the information.
In Marieholm, the staff considers that they get the information they need. This information is distributed to them at meetings arranged by the unit manager. There is also access to paper-based documents if the oral communication is lacking. They emphasise that the oral information is much easier to adapt than the paper-based information.

In Timmersdala/Lerdala, the staff considers that the information they need is lacking. There are meetings where the information is distributed but they are not regular and even if there are documents, they are not read depending on lack of time. In the future they hope that the intranet of the municipality will be an opportunity to distribute information in a more efficient way.

**How is unauthorised access prevented in the care-receivers’ records? What are the needs in order to improve that protection against unauthorised access in existing and future systems?**

In Marieholm, with a manual system for the care-receivers’ records, the staff considers that the protection against unauthorised access is sufficient. There have been no incidents, neither externally nor internally, where records have been objects for unauthorised access. The interest for those care-receivers is not large in common and the members of the staff have no time to read records they do not have access to.

One staff nurse considers that there are files with medicine lists, which are left about at the care department. It happens that the care-receivers themselves can read the medicine lists of other care-receivers and that is not the purpose. The staff nurse considers that this deficiency must be improved. The unit manager, who has access to the computerised system, must be logged in to the intranet with her username and password if the other persons in the staff will be able to do the orders of material. This is not satisfactory either, the unit manager considers, but it will be better when the staff nurses have got their own computers and their own user names.

Neither in Timmersdala/Lerdala, with the computerised care-receiver record system, have there been any incidents where records have become objects for unauthorised access. The staff is yet uncertain about the risks of unintentionally internal unauthorised access, because the levels of authorities are not clearly prepared. Today all nurses in the municipality can read the records. The nurses want clearer and more defined blocks.

Even the unit manager and the MAS consider that the protection should be able to be improved, above all, the levels of the authorities. The MAS considers that it is acceptable that all occupational groups being under HSL have access to all care-receivers’ records in the municipality, but he questions if they must have access to all parts in the record.

Regarding encrypted systems there is none of the respondents, neither in Marieholm nor in Timmersdala/Lerdala, who really know or have got information whether the systems are encrypted or not. They suppose so, but they have no knowledge about it. They thought they knew that the facsimiles are not encrypted and here all personal groups mean that there are lacks. There exist many transformations of sensitive information by

---

5 HSL is a Swedish acronym for the Act of Healthcare. In Swedish: hälso- och sjukvårdslagen
facsimiles and it would be unfortunately if this information got in wrong hands. There are
guidelines introduced such as give a call back at such a sensitive information
transforming exists but this requirement does not ensure the information is transformed
to the right receiver. If the information has gone astray way, it is already too late to do
something about it.

**Are there any clearly compiled levels of access? Are there any persons in charge
managing the authorities up-to-date?**

In the manual system in Marieholm, it is just the nurse who has the access to the records.
There is still no checking to confirm it, but there exist no suspicion that it is not
followed. Today the nurses have only access to the records in their own geographical
unit, which is a disadvantage when the nurses have their evening shift. Then the whole
municipality is their working area.

In the computerised system in Timmersdala/Lerdala, there are levels of authorities
between the part of the record standing by the HSL and the part standing by SOL\(^7\). They
consider that these levels of authorities are satisfactory. On the other hand there are no
differences in the levels of authorities between the occupational groups in the part of
record standing by the HSL. The nurses have access to e.g. the whole records of the
occupational therapist and vice versa. The levels of authorities are under consideration
and the largest problem is in this context the administration of the authorities. It is the
responsible person of the system who is in charge of up-to-dating the authorities and the
staff’s experience is that it is satisfactory. It is a greater problem that there are new
employees with no user names than there is a problem with too old user names in the
system. Deputies and employees by the hours generate a larger amount of administration
of authorities and lead to problems in computerised systems.

**Are there any routines for following-up the information security in the
organisation?**

In general, for both the manual system and the computerised system, none of the asked
persons consider that there are any routines for following-up and evaluating the
information security.

In the manual system the information security mostly concerns about the secrecy and the
duty of silence. Discussions about the information security exist most often at meetings,
but it is almost the staff itself that brings the question up. The context of information
security is also up-to-date when summer-deputies are employed. The staff in Marieholm
considers that there is no following-up or evaluation of the information security.

In the computerised system there is a block in the system forcing the users to change
their password after a fixed number of days. This seems to be a good support but there is
still a problem with repeatedly changing the passwords, because the password must be
managed in a safe way. The staff thinks it is hard to remember the password, which gives
rise to writing the password on separate notes, which are not satisfactory managed.

---

\(^7\) SOL- a Swedish acronym for the Act of Social service. In Swedish: Socialtjänstlagen
There is no evaluation or following-up about how the users manage the passwords or moreover, how the information security is managed according to the staff.

**Is there any existing educational programme in the organisation in order to educate the healthcare staff in information security policy?**

There is no specific educational programme for information security, neither in Marieholm nor in Timmersdala/Lerdala. In Marieholm, where they shortly will introduce a computerised system, they are delighted to include education in security in the ordinary educational program for the computerised system. Today it is not in the educational plan.

Neither the computerised system in Timmersdala/Lerdala has any specific educational program occurred. In the education of the computerised system some questions of security is arisen in the context of user names, passwords etc., but regarding to the staff it is more common that the users themselves ask these questions than it is included in the educational programme. Regarding to the MAS, the thought is that some education in the security context will be a part of the further education of the system, but frequently there are other priority questions in these occasions. The problems with the information security will be extended the day when the staff nurses are going to use the system. Today, there are already many different interpretations about questions of secrecy and it is likely not decreased when there are more participant users, according to the MAS in Skövde.

**Is sensitive information in the system logged? How is the log checked and managed?**

In the computerised system, information has been distributed to the users that the system is logged. It was not until the turn of the year 2000/2001 the logging was realised and there are still no routines for checking the log file. The log has only been checked two times. Neither, has any information been distributed to the users about what kind of data is logged, just only that the system is logged. None of the asked persons knew what kind of data is logged about them in the log file.

**Other questions applied from the observations**

- The staff nurses consider that the most important information which would have negative consequences if it goes wrong, are above all the medicine lists and information about the treatment. They also mention other types of information such as: what kinds of aid the care-receiver has, the relatives’ telephone numbers, addresses to the pharmacy, taxi etc, and also the historical background of the care-receivers.
- These types of information mentioned above, the staff nurses also declare as sufficient and necessary, and will be needed in a possible mobile system. The staff nurses also mention the opportunity to see what services the care-receiver is allowed to, as an important source of information. The connection to other occupational groups as occupational therapists and physiotherapists are mentioned as an improvement of the correctness of the information when the system is computerised. The nurses also consider that personal data is important data to have in the field particularly in emergency situations. In general, the staffs in both Marieholm and Timmersdala/Lerdala are positive to mobile units but they also emphasise that it must
not replace the oral communication between the staff, which they consider is very important to the work but also socially.

- Regarding to the archiving of the records, in Mariestad they have decided a storing time of ten years. This implies that old records are sorted out. The nurses send finished records to the MAS who archive them. Therefore, there are only up-to-date records at the nurses’ expedition. The municipality in Mariestad have the purpose to store paper-based copies of prospective computer records in the future. But they consider that there are many unclear aspects and archiving is a challenge for the future.

- In the municipality of Skövde, all records are preserved in the system at each administration unit. There is a suggestion to create two new administration units; one for the deceased and one for inactive care-receivers. Today there is no sorting-out time in the municipality but a ten-year-plan is under discussion. One of the problems with computer records is the storing device in which the data is to be stored in. There have been discussions about making paper-based copies of all records and then store them in a traditional way.

- The unit managers have answered the question about how the staff nurses are going to be integrated in the record system. They consider that this development will come in the future but it is important to emphasise questions such as secrecy, security and also the usefulness of it. In the first place, they think stationary computers are of interest. It will be a long time before the mobile computer units are available for the staff nurses.

- Medicine lists are an important source of information. In Mariestad they have no plans to enter the lists in a manual way in the coming computerised system. Possibly, the information can be scanned in the future but is not current in the present situation.

In Skövde they have tried a routine implying that, at the units, which do not have any evening working nurses, the medicine lists are entered in the system manually. The nurses have protested against the routine because there is no time for such registration and there are no guaranties that the entered information is correct. The developers of the system have plans to integrate the systems between the municipalities and the Pharmacy Company for having access to the medicine lists in a digital form. Today, it does not work sufficiently, according to the nurses.

- In Skövde, the computerised system has access to the register of national registration. The nurses consider that this is a support in the work when they do not have complete personal data of the care-receivers. The current civil status can be one example when this information has importance for the correctness of the information.
5 Synthesis

It is not a news-item that there are lacks in the information security within the healthcare. The DIB points out in their report (Datainspektionen, 1998) that the computerising in Swedish healthcare is widespread. In spite of healthcare by tradition being very anxious about the patients’ integrity and defending their secrecy, there are still deficiencies in the management of the patients’ healthcare data in computerised systems.

This work has its focus on the home healthcare, with the municipalities as the responsible authority. The examinations of the DIB have been intended for the hospitals where the county councils are the responsibility authorities. It is therefore interesting to see, that within the home healthcare with the municipality as the responsible authority, there exists the same kind of deficiencies that in the healthcare where the county councils are responsible. It can also be pointed out that the basic strategies for the information security, especially the IT-strategies, are worse in the municipalities than in the county councils. Both municipalities focused on in this work, have deficient IT-strategies. In one of the municipalities it has been impossible, on the whole, to have access to any IT-strategies. According to reports, they are in the process. In the other municipality, there is a proposal presented to the Municipal Executive Board about developed IT-strategies but these are very general and are more on an all-embracing level, far away from practical guidance for the users who use the systems in their daily work.

Whether the systems are intended for care or not, the basic strategies for manage the systems are deficient or not even existing. This implies that there are already deficiencies in the information security on a basic level. Strategies must exist for basic functions like back-up routines, virus protection, cryptographic techniques, fire security etc.

From the realised work, there are three points, which should be held up as apparent deficiencies in the information security. These points are education, levels on access profiles and facsimile transmissions as information distributor. Below, there is an account of these three points.

5.1 Education

When an information system is going to be developed, apart from the fact that it is a system of care or not, it is important to take the whole life cycle of the information system in consideration. In most cases, great resources are spent on analysis, design and implementations. Also acquisition of hardware is a very expensive effort. Then, when the system is introduced in the business, the allotment of resources for education falls short. One decisive factor is the gains with a fast introduction of the new system. Within healthcare there are many employees of different categories. To have gains in form of better and cheaper care for the patients it will be required that all actors in the whole care chain can use computerised support in their work. In consequence of this, the numbers of affected persons who are going to have education are extensive. In literature and other documents the importance of education is emphasised.
Van Bemmel & Musen (1997) mentions that throughout the world, healthcare professionals generally lack knowledge of the possibilities and limitations of systematically processing data, information, and knowledge and of information technology. They are often asked to use computer systems of which they have limited appreciation, which could enhance their practices substantially via better use of information resources. It will only be through improved education of healthcare professionals and through an increase in the number of well-trained workers in medical informatics that this situation can begin to reverse itself (van Bemmel & Musen, 1997).

Perhaps the most important pillar, upon which any serious effort towards introducing and enforcing security in healthcare information systems is based, is the level of awareness (or knowledge) that those responsible for managing the effort have. Thus, the issue of proper awareness, training or education of healthcare management is of paramount importance (Katsikas, 2000).

Theoretically, many people agree with the importance of education. However, it is hard to see the practical realisation of education in practice. In spite of this, you may see advantages with a quick introduction of information systems in the business (Petersson & Rydmark, 1996).

Concerning education of information security, there are no direct gain advantages, which can be clearly found in the budget. Here there is another set of values than clearly economical, which must be observed in the first place. If it is hard to reserve resources for education when economical gain advantages can be obtained, the question must be asked how important it is to give education in information security, which cannot directly give such advantages. When the personal integrity and the protection of defending the secrecy are emphasised as an important part of the education, there are great risks to not give necessary allotments of the resources for this purpose, despite the legislation being clearly defined in this question and despite many recommendations and common advice existing to realise the security routines in the business.

This work has pointed out that education has clearly fallen short regarding information security in both the computerised and non-computerised systems.

5.2 Levels on the access profiles

The access profiles are the parts of the access control system where different actors are defined and how they are allowed to process the information. In the existing access control systems there are differences concerning how sophisticated profiles they may create. To maintain a suitable level of information security for patient information two models are most often combined; the access model and the logging model. More specific description of the models is found in section 2.4.

In this work, the computerised system in Skövde has practiced the logging model, which implies that all nurses have got the same access to all care-receiver records in the municipality irrespectively of the fact which unit they are working at. The logging model implies access on one’s own responsibility. According to the SITHS-group, it is important for this kind of method that there exist systems and administration to follow-
up the logs (Björner, 2000). There are differences between different care organisations how much resources can be reserved for administration in the models respectively. In most cases, one of the models is given priority to the expense of the other, according to Björner (2000). Some care organisations can have clearly prepared and individually adapted access profiles, which take a lot of time to administrate at the same time as the following-up routines for the log is maintained to a limited extent. Other organisations have very “wide meshed” access profiles instead, which take less time to administrate. Instead, the greater part of the resources is reserved for following-up the logs (Björner, 2000).

The principal aim is to develop and implement need-to-know access-controls that would protect patients’ healthcare data. The user would only be allowed to access information necessary to complete his or her job (Smith & Eloff, 1999). This is also associated with The Act of Secrecy.

The risk with the logging model is proclaimed to be obvious, which has also been shown in this work. The logging model is used to give all the users access on their own responsibility while, in lacks of resources, there are still no routines for checking the log file. The municipality of Skövde has got their computerised record system for more than one year. However, during the first six months the log has only been checked two times (Åhlfeldt, 2001b). Considering the sensitiveness of the information managed in patient record systems, the access model is to prefer despite the amount of administration it requires. Perhaps the best practice would be to have a combination of the both models.

5.3 Facsimile as information distributor

Personal data from the municipalities to the institutional care is in most cases transformed by a written document sent with the patient. The transformation, occurring from the institutional care to the municipality or the primary care, is however mostly performed by facsimile transmissions. In some cases, some documents are transformed by the patients themselves or by mail. In both municipalities investigated, these documents are very often transformed by facsimile in a common way. The information can be exposed to many threats when the facsimile transforms it. The DIB gives some examples of such threats in their report (Datainspektionen, 2000:2).

- the document is sent to a wrong receiver because wrong receiver-number is used
- the document is received by wrong person at the receivers place depending on lack of routines at the latter
- unauthorised people can have access to the document depending on an unsuitable placing of the equipment.
- the equipment can be exposed to unauthorised manipulation for the purpose of changing a document or sending a document to an unauthorised receiver.
- technical interferences in the telephone connection can lead to lost or unreadable documents.

The DIB also considers that it is important for the organisations to have a clearly well thought-out and prepared security policy. The protection is to be adapted for the own organisation and for the extent of the sensitive information (Datainspektionen, 2000:2).
When computerised systems for patient record documentation is implemented in the business, there are guiding principles and demands on how the personal data is to be protected in electronic transformation. Generally, the staff does not use common e-mail at transforming personal data, instead they use functions in the patient record system that, according to reports, would be encrypted. This is a good security measure but there are risks when only the computerised systems are in focus for security thinking, while in the daily work there are other types of information systems as the facsimile, which transform sensitive data about the patients without even raising the eyebrows of the staff and propose calling the security risks in question. Most often this handling depends on deficient information and awareness about the risks. Simple measures can be performed to manage the deficiencies without costing too much.

Below, some of the measures performed by the DIB for transforming personal data by the facsimile within the healthcare of old people, are mentioned (Datainspektionen, 2000:2).
- analysis of the vulnerability should be performed in order to pay attention to those people with the over-all responsibilities about the threats and the need of security measures when using the facsimile.
- at purchasing the facsimile equipment, a solution with functions which are adapted to the own need of the organisation should be chosen.
- the functions, short number and name memory, should be used to minimise the risk of using the wrong subscribe number at transmissions
- the facsimile transmission should be encrypted if there are risks that the transformation would be tapped.

Other technical solutions are also conceivable to minimise the security risks. There is a realised project, which implies that the district nurse by her mobile telephone gets a message telling that she has a personal fax from e.g. the medicine clinic. By dialling a personal code, she can get the fax from the nearest facsimile. The evaluation of this project is stated to be positive. Besides, the accessibility is facilitated when the fax message can be derived at the nearest facsimile (Datainspektionen, 2000:2).

5.4 Comparison between the manual and the computerised patient record system

The difference between a manual system and a computerised system regarding information security is that the risk for deficiencies in the information security increases in connection with computerising the patient record system. In the computerised system in Skövde all nurses have access to the care-receiver records in the whole municipality, which implies that the risk for internal unauthorised access increases. In the manual system in Mariestad, it is only the district nurse who has got access to the care-receivers’ records. For this reason the records are not available for other care-performers than herself, why spreading of care-receiver records to other places is not any problem. Besides, it implies that the records are always locked up in the district nurse expedition where no other has entrance at which the risk for internal unauthorised access is reduced. The disadvantage with the manual patient record system is on one hand; it can be hard to
have the patient record accessible when it is needed but also, the patient record can be accessible both for external and internal unauthorised access. In this work, it has shown up that the risk for external unauthorised access is not big, neither for the manual system nor the computerised system. On the other hand, there is always a risk for internal unauthorised access.

There are deficiencies regarding education and transforming of information by facsimile in both the manual and the computerised systems.
6 Possible future research

From the synthesis above, two things can be pointed out for future research. It is education and access levels.

6.1 Future research regarding education

People speak a lot about the importance of education in order to have functional, effective and secure information systems. An interesting future research aspect would be to select a homecare unit in a municipality presently in an introduction phase to a computerised patient record system. Give the users all the education, both functionally regarding the application and in information security that is considered to be sufficient and necessary. After some years, when the education has been realised and the system has operated for a while, make a survey to see what education in information security has meant for the information security and if it has been improved. It would also be of interest to make a general estimation on how big resources are needed to get a good security education. This could be an incitement for other municipalities standing in an introduction phase for a computerised system.

6.2 Future research regarding access levels

Since the ”Ädelreformen” came into force, in the turn of the year 1991/1992, the municipalities are responsible for giving people in special livings a proper care and planning healthcare from the basis of the citizens’ needs of such care. Therefore, the municipalities do not have any long experience of handling care information and have not kept up with the development of systems handling this information. Administration of authorities is a problem in the municipalities. There is a large turnover of employees and there are different categories of appointments with different geographical reach. It is unfortunate to choose a more open strategy for authorities only because the administration of the authorities is a burden. This is not a problem only for the systems of care. The administration problem of authorities also concerns information systems in general.

One interesting future research aspect would be to find out in what way the administration of authorities can be facilitated. We must not come to the situation that we build computerised systems to facilitate the ordinary administration and then come to another form of administration, almost with the same burden and performed in a manual way. There should be opportunities to see if the allotment of the authorities could be delegated out into the organisation so it will not be so heavy to only a few persons. Furthermore, the administration of the authorities should be automated with the help of computer support in order to increase the capacity of the administration.

The SITHS-group gives one example of such a function in their rapport (Björner, 2000). They mean that the manual administration of handling the authorities give rise to problems when care performers is occupied in more than one role, a typical example is doctors of duty. They mean that it would be desirable to integrate the access control system with systems containing information about the different roles of the care performers in order to get it all to work in a dynamical way.
Another future research aspect is also to find out if other kinds of identification techniques than user-names and passwords are a possible to have at hand even for municipalities and their care-systems. Today, there are techniques for smart cards and other bio-technical items as fingerprints, iris-recognizing etc. Today, these techniques are limited because they are expensive but in the view of research, it would be interesting to find out how these techniques could ensure the accessibility to the systems without making great demands on the users. Facilitating the management of user names and passwords should be a measure to strive for.
7 Concluding remarks

The aim of this work was to survey the security problem concerning personal integrity and secrecy in systems managing personal data in the home healthcare from the basis on the recommendations and common advice for processing of personal data compiled by the DIB. The result of the work has shown that there are security problems like inadequate education in information security and deficiencies in the levels of access. In addition, the work has even shown that transforming of information by facsimile is deficient.

Furthermore, it must be notified as there are not any clear IT strategies in the municipalities in order to get a foundation to build the information security on, the possibility to get sufficient information security is minimised.

Furthermore, the aim with this work was to find out how existing and future systems can support the users in fulfilling the recommended security requirements.

According to education the need is not on the first hand how the system can give support to the users. It is a bigger need of resources at a higher level so there are opportunities to education for the users, partly to learn the systems but also education in information security and security awareness in general. These needs are not dependent on technique but of course the techniques can be used to mediate information to the users about current acts and directions, for example.

According to the access profiles the levels of access in the system should be on a level, which gives the users safety when using the system. It should not be the user’s responsibility to decide what information the user has access to. Today, the technique has the opportunity to give satisfactory support to the users, but then it needs to be implemented in the systems. The routines that administrate the authorities should be revised. Besides, the administration should be analysed how it can be delegated out into the organisation.

According to the transformation of information by the facsimile, these deficiencies can be measured effectively by consciously realising the risks which this kind of transforming lead to. If the existing recommendations are accepted a satisfactory information security can be performed when the facsimile transforms personal data.

Security is an important part of the protection of the personal integrity. A satisfying security is a demand according to The Personal Data Act. Security is not something extra. Security is a normal part of doing business.
References


Appendix

Glossary of terms and abbreviations

**DIB**
An abbreviation used in this thesis for the Data Inspection Board

**HSL**

**KSS**
A hospital in Skövde

**MAS**
A Swedish acronym for medical responsible nurse, in Swedish: medicinsk ansvarig sjuksköterska.

**Primary care**
The first level of care comprising basic medical investigation, treatment and care.

**SOI**

**The Act on Healthcare Record**
A translation from the Data Inspection Board for the Swedish word “Vårdregisterlagen”.

**The controller of personal data**
A translation from the Data Inspection Board for the Swedish word “personuppgiftsansvarig”.