INTRODUCTION TO INFORMATION SECURITY

For non-permanent and external staff: consultants, temporary staff, students, tradespeople and others.

Introduction

This document is intended for non-permanent and external staff. The term non-permanent and external staff refers to people who are not employed directly by Region Halland, usually consultants, temporary staff, students, tradespeople and similar. In conjunction with them being briefed about the workplace, the client, manager or other designated person must ensure that the external staff member has read and understood the content of the Introduction to Information Security. Receipt of the document must also be confirmed by providing a signature. This signed confirmation is filed by the client, project manager or other relevant staff.

Information security

Everyone who works at or performs an assignment for Region Halland must have read, understood and accepted the content of the Introduction to Information Security.

To ensure adherence with the confidentiality obligations of the healthcare and dental care providers, and regarding other areas of the region's activities, and to ensure the observance of general security guidelines, all users must comply with these regulations.

Information security policy

Region Halland has a *security policy* (swe) that includes information security.

Permissions

The Head of Administration / Head of Operations (or equivalent) is the information owner and is responsible for defining and assigning access permissions. This applies in the case of new employees, new students, changed assignments or work tasks, as well as absence.

Group logins mean that several people use a common login identity. These may be used as an exception in locations where a small number of computers are used by several people. Each individual who logs in is responsible for their own activities. Group logins allow limited access to functions in the region's IT network.

IT and production environment

Subcontractors who do not have operational responsibilities must inform the IT manager about the purpose and point in time of the access, and any planned changes, before logging into the region's production environment.

Your computer

General

It is prohibited to connect computers that have not been set up by the
IT Service to the region's network.

Any suspicion of viruses in programs or data files should be reported to the IT Service immediately.

Any requirement to install programs or extensions to programs is the responsibility of the immediate manager, who takes care of this in accordance with the system administration model.

Temporarily leaving the computer unattended
Computers that are left unattended should be locked.

At the end of a work session
Log out from the network at the end of a work session. Turn off the computer at the end of the working day, unless someone else is to use it, and also turn off the monitor.

Clean up the computer's desktop
Do not save documents directly on the computer's desktop. Documents should only be saved in the designated folders.

Email

Emails are covered by the same rules concerning publishing, confidentiality and archiving etc. as is

the case with traditional letters and fax communications. Each employee's list of emails, i.e. details of the email address, sender, recipient, subject heading, and dates in the inbox and outbox, are public documents.

Your email address (…@regionhalland.se) may not be used for non-work correspondence. Contacting patients and sending information to them via email is not permitted. Information covered by confidentiality, such as patient records, must not be sent using normal email. Only secure email channels may be used for such purposes.

Personal identification numbers may be sent by email, but never along with information considered to be private, such as healthcare information or personal assessments.

See the Email (swe) procedure.

Video meetings

Particular care should be taken when the share desktop function is used, as everything displayed on the screen, such as patient records, becomes visible.

See the *Video conference and chat (swe)* procedure.

Internet

The *Internet use by staff* (swe) procedure describes how to act when surfing online.

Storage of information and storage structure

The information in our IT systems and storage units belongs to Region Halland and should be work-related. The G and H drives are sometimes perceived as being for personal files, but it is not permitted to save music files or documents of a personal nature (such as photos) in any of the region's storage areas. The IT Service is allowed to delete files of this type that are saved on the H drive. Using the region's storage space for files that are not work-related can lead to disciplinary measures being taken.

It is not permitted to store information in cloud services with which Region Halland does not have an agreement (e.g. Dropbox, iCloud, Google Drive).

Patient data
Patient data, including photos, must not be stored on any of the drives listed below; such data has to be stored in special healthcare systems or, as an exception, on a CD (digital images).

C drive
The computer's hard drive should not be used for storing documents. No backups are made of it.

G drive
Company-wide documents and files are stored here.

OneDrive
Storage area in the cloud. Used to store and share information. May not be used for handling sensitive or confidential information.

Collaboration sites/Teams
Information that needs to be shared by multiple people can be stored at collaboration sites. Collaboration sites are intended for members of projects, management groups, network groups, etc.

Checking of logs and unauthorized access to data

Checking by the employer

The employer has the right to monitor and check all the information stored in the region's IT system (including emails). The management can therefore check what is stored in the region's storage areas at any time.

Checking logs

The Head of Operations or equivalent, who is authorized to decide about the access permissions that are granted, is responsible for regularly checking the logs in accordance with the defined procedure.

Unauthorized access to data

Accessing the records of a patient with which you do not have a healthcare relationship, unless the information is needed for a special assignment, is considered unauthorized access to data/a breach of confidentiality. If when the logs are checked it emerges that you have accessed data without having the relevant authorization, this may be reported to the police or disciplinary measures may be taken.

See the procedure Suspected unauthorized access to data, breach of the duty not to disclose information, IT sabotage. (swe)

Public access to information

The Freedom of the Press Act is one of Sweden's fundamental laws. It gives citizens a unique insight into the activities of all public bodies, and is often called the principle of public access to information. This puts special demands on public sector employees, such as us. We must ensure compliance with the law, so that everyone has the opportunity to exercise their democratic rights. The Freedom of the Press Act is one of our most important laws and regulates how information is handled by public authorities, including everything from making case notes and records to filing documents. In this particular context, the authority is the political board/operational board in Region Halland and the administrative area is the authority area.

The Public Administration Act contains requirements regarding the provision of service and the handling of cases.

Confidentiality and the duty not to disclose information

The Public Access to Information and Secrecy Act (SFS 2009:400) contains provisions on confidentiality relating to public authorities. The general rule is that all public documents are made accessible to the public. Examples of exceptions include patient records, which are public but confidential documents.

In order to protect the personal privacy of patients, confidentiality in the healthcare sector applies to information about an individual's health status or other personal circumstances. Confidentiality means that it is forbidden to disclose information, whether verbally, in writing, by disclosing or showing documents or in some other way. Confidentiality does not apply if the information can be disclosed without the individual or any relative feeling uneasy about it; in other words a confidentiality assessment must first have been carried out in such cases.

Confidentiality may also apply to other documents, such as procurement documents, administrative staff documents containing information about an individual's personal circumstances, information relating to union negotiations and the results of risk analyses that have been performed.

Confidentiality regarding the public population register

Information stored about people in the public population register, such as name, address and personal identification number, is usually publicly accessible. In some cases, it is important to prevent what would normally be harmless information from being disclosed. Such a case could be if a person is exposed to a threat and has therefore had to make their personal data in the public population register confidential.

Region Halland normally only makes personal data held in its registers confidential if it relates to a person who has had their personal data made confidential in the public population register, although there are some exceptions to this (chapter 21, section 3 of the Public Access to Information and Secrecy Act)
See the procedure Confidentiality regarding the public population register (swe)

Personal data and data protection

Personal data does not necessarily mean a personal identification number; it is sufficient that the information can be linked to a particular individual.

The General Data Protection Regulation states that legal basis is required in order to register personal data. Region Halland is permitted to register personal data on various legal bases, for example if this is necessary for establishing a contract of employment between you and the employer or if the employer has a legitimate interest in processing the data. More information about how your personal data is processed is available in *Personal data – information for employees*. (swe)

Data Protection Officer

The political boards responsible for personal data appoint Data Protection Officers (DPO), who have the task of ensuring compliance with the requirements of the General Data Protection Regulation. Among other things, DPOs maintain a list of personal data registers and approve applications for the creation of new registers.

Appendix

Appendix: Confirmation of receipt: Introduction to Information Security

Appendix - Confirmation of receipt: Introduction to Information Security

Confidentiality
Confidentiality means that you are not allowed to tell people about or disclose information about a patient to anyone other than the people providing care to the patient – you have a duty of confidentiality regarding the information to which you have access.

You must therefore not discuss an individual patient's health or other personal circumstances with anyone who is not involved in providing care or treatment to the patient. This applies even if the other person is also bound by a duty to observe confidentiality.

The obligation to maintain confidentiality also applies even after you have stopped working in the healthcare sector i.e. forever.

It is not a given that information about a patient should be disclosed to that person's relatives. Ask what the patient wants in this regard or check if documented consent is available in the medical records. It should not be disclosed that a patient has been admitted to a healthcare ward or department, unless it is clearly stated that this information can be disclosed.

You are also not entitled to access documented information about patients unless you are involved in caring for the patient or otherwise need the information to perform your work. There are exceptions to this general rule. In some cases, you are required to disclose information that is classed as confidential. If you are uncertain, you should contact your immediate manager or the region's lawyers.

What information is classed as being confidential?
Confidentiality covers, for example, information about the identity of the patient, the patient's illness and treatment, the patient's address details, information about the patient's family situation and other social aspects, possible incapacity for work, employers and more.

Such information is often stored in patient records or in notes kept in other ways, but confidentiality also applies to anything that patients or their relatives tell the staff.

Who is covered by the Public Access to Information and Secrecy Act?
The Act applies to all employees in the healthcare sector, regardless of their position and duties. The confidentiality obligation also applies to students and trainees.

Breaches of the duty not to disclose information

Breaches of the duty not to disclose information are covered by public prosecution and can result in fines or imprisonment of up to one year. More information about confidentiality obligations is available on the intranet at Intranätet/Rutiner/Sekretess och samtycken (in Swedish).

Confirmation of receipt
I have read and understood what is meant by confidentiality and the duty not to disclose information, and have read and accepted the contents of the Introduction to Information Security.

I undertake to check for and take note of changes and new developments in this area in the future.

I undertake to only access documented information about a patient if I am involved in providing care to the patient or I need the information for some other reason as part of my work assignment. I also pledge that I will not in an unauthorized way disclose to a natural or legal person the information about which I become aware during my assignment for Region Halland.

.....
Date

.....
Signature

.....
Name in block capitals and personal identification number

The filled-in confirmation of receipt is stored at the client for 70 years, preferably in a binder or in the client's annual file (official register)

Updated from previous version
Storage device H: is deleted