Non-disclosure agreement

Background
The principle of confidentiality aims to safeguard private interests and is rooted in the desire to protect individuals' personal circumstances and private sphere. Confidentiality is a key aspect of data protection.

Confidentiality is also necessary in order for patients to be able to place their trust in the health service and approach the health service to receive treatment. If healthcare staff and others did not have to observe confidentiality, it could prevent patients or their next of kin from seeking help for fear of information being passed on.

Scope
The duty of confidentiality applies to information that the signatory learns of in the course of their work concerning health and medical conditions, information about other personal circumstances, information about technical equipment, methods and competition-related business matters, information pertaining to data security and information that must be kept confidential for other reasons.

The duty of confidentiality continues to apply after the service or work has been completed.

For more information about confidentiality in the health and care services, see:
https://helsedirektoratet.no/taushetsplikt/taushetsplikt-i-helse-og-omsorgstjenesten

Statutory regulations
The following describes statutory confidentiality clauses

- Pursuant to Section 21 of the Health Personnel Act, health personnel are obliged to prevent others from obtaining information about people's health or medical conditions or other personal circumstances that they learn of in their capacity as healthcare workers. Nor may such information be read, sought or possessed except when the provision or administration of healthcare requires it or if otherwise permitted by statute.
- Pursuant to Section 6-1 of the Specialist Health Service Act, anyone providing services on behalf of health institutions covered by the act has a duty to observe confidentiality pursuant to the Public Administration Act Section 13.
- Pursuant to Section 15 of the Personal Health Data Filing System Act, anyone processing health data under the act has a duty of confidentiality.
- Pursuant to Section 17 of the Personal Health Data Filing System Act, anyone processing health data under the act has a duty of confidentiality under Section 21 of the Health Personnel Act.
- Pursuant to Section 3-6 of the Patients' and Users' Rights Act, information about health and medical conditions and other personal data must be treated in accordance with prevailing legislation on confidentiality.
- Pursuant to Section 13 of the Public Administration Act, anyone providing services on behalf of an administrative agency is obliged to prevent others from obtaining information about personal circumstances and about technical equipment, methods and competition-related business matters that they may learn of during the course of the service.

Breach of confidentiality
Pursuant to Section 67 of the Health Personnel Act, breaching the provisions of the act, including its confidentiality clauses, is a punishable offence.

Pursuant to Sections 209 and 210 of the General Civil Penal Code, it is a punishable offence to breach confidentiality imposed in pursuance of legislation or valid instructions.

The enterprise considers a breach of confidentiality to be a dereliction of duty or a breach of contract with the health trust. A breach of confidentiality may have consequences for any employment or contract.

Declaration
The signatory is familiar with the statutory duty of confidentiality that must be observed, including which information is subject to confidentiality, and that a breach of confidentiality may result in criminal liability. The signatory is also aware that Helse Vest IKT considers a breach of confidentiality to be a dereliction of duty / breach of contract with the enterprise.

Date of birth	Signature	Name in block capitals
(D.o.B.)		(Name)

HELSE VEST IKT

Non-disclosure agreement – Appendix to form

Overview of relevant legislation

Act of 2 July 1999 no. 64 relating to health personnel etc. (Health Personnel Act)

Section 21 – General rule relating to the duty of confidentiality

Healthcare staff shall prevent others from gaining access to or knowledge of information relating to people's health or medical conditions or other personal information that they learn of in their capacity as healthcare staff.

Section 21a – Unlawful appropriation of confidential information

It is illegal to read, search for or in any other way obtain, use or possess such data as described in Section 21 unless it can be justified in relation to the provision of healthcare to the patient, the administration of such care, or if another act or regulation expressly permits it.

Section 25 – Disclosing information to co-operating personnel

Unless the patient objects thereto, confidential information may be given to co-operating personnel when this is necessary in order to provide appropriate healthcare. Nor shall the duty of confidentiality pursuant to Section 21 prevent personnel assisting with electronic processing of such information or providing servicing or maintenance of equipment from gaining access to such information when such assistance is necessary in order to comply with statutory requirements for documentation. Unless the patient objects thereto, confidential information may be disclosed to co-operating personnel when this is necessary in order to provide appropriate healthcare, cf. Section 10 a.

Personnel mentioned in the first, second and third paragraphs are subject to the same duty of confidentiality as healthcare workers.

Section 26 – Providing information to the management of an enterprise and to administrative systems

The healthcare practitioner may disclose information to the management of the enterprise when this is necessary in order to provide healthcare or for the purposes of internal controls or quality assurance of the service. The information shall be given without identifying characteristics whenever possible.

Such information may also be disclosed to the management of the co-operating enterprise when co-operating on treatment-based health registers pursuant to Section 9 of the Personal Health Data Filing System Act. The healthcare practitioner shall not be prevented by the duty of confidentiality pursuant to Section 21 from providing the patient administration of the enterprise with details of the patient's national ID number, information relating to diagnoses, any assistance required, services offered, admittance and discharge dates as well as relevant administrative data. The provisions relating to the duty of confidentiality shall apply correspondingly to personnel employed in patient administration.

Section 45. Disclosure of and access to patient records and information therein

Unless the patient objects thereto, healthcare staff providing patient services under this act shall be given requisite and relevant health data when necessary in order to provide appropriate healthcare to the patient. It shall be evident from the patient records that other health personnel have been given access to the records. Health data described in the first paragraph may be provided by the data controller in charge of the data or by the healthcare staff who documented the data, cf. Section 39. The Ministry may in regulations stipulate further provisions to supplement the first paragraph and may include among them that other healthcare staff be given access to patient records, including in cases not described in the first paragraph.

Section 67 – Punishment

Anyone who intentionally or by gross negligence contravenes the provisions of this act, or who aids and abets thereto, shall be punished with a fine or a term of imprisonment not exceeding three months. Public prosecution will be instituted if it is in the public interest or by petition by the Norwegian Board of Health Supervision.

Act of 2 July 1999 no. 61 relating to specialist health services etc. (Specialist Health Services Act)

Section 6-1 – Confidentiality

Any person carrying out services or work for health institutions covered by this act is obliged to observe confidentiality under the Public Administration Act Sections 13 to 13 e.

The duty of confidentiality also extends to a patient's place of birth, date of birth, national ID number, nationality, civil status, profession, home address and place of work. Information about a patient's domicile may still be provided if it is evident that the disclosure will not negatively affect trust in the health institution.

Data may only be given to other administrative agencies pursuant to section 13 b, nos. 5 and 6, of the Public Administration Act when this is necessary in order to help solve tasks under this act or in order to prevent a significant risk to life or serious damage to health.

Act of 20 June 2014 on personal health data filing systems and the processing of personal health data (Personal Health Data

Filing System Act)

Section 17 – Duty of confidentiality

Any person who processes personal health data pursuant to this act has a duty of confidentiality pursuant to the Health Personnel Act Sections 21 et seq. Others who obtain access to or knowledge of health data from health data filing systems have the same duty of confidentiality.

Section 18. Unlawful appropriation of confidential health data

It is unlawful to read, search for or in any other way obtain, use or possess health data processed under this act unless another act or regulation expressly permits it.

HELSE VEST IKT

Non-disclosure agreement – Appendix to form

Act of 2 July 1999 no. 63 on patients' and users' rights (Patients' Rights Act)
Section 3-6 The right to protection against the dissemination of information
Medical and health-related information and other personal information shall be treated in accordance with the prevailing provisions regarding confidentiality. The information shall be treated with caution and respect for the integrity of the person whom the information concerns. The duty of confidentiality shall cease to apply if the person entitled to confidentiality consents to it. If healthcare staff make available information that is subject to a statutory duty of disclosure, the person whom the information concerns shall, so far as is warranted by the circumstances, be informed that the information has been disclosed and of the nature of the information in question.

Act of 10 February 1967 relating to procedure in cases concerning the public administration (Public Administration Act)
Section 13 – Duty of confidentiality
It is the duty of any person rendering services to or working for an administrative agency to prevent others from gaining access to or obtaining knowledge of any matter disclosed to them in the course of their service or work concerning:
1) an individual's personal affairs
2) technical devices and procedures as well as operational or business matters which for competition reasons must be kept secret in the interests of the person whom the information concerns

The term "personal affairs" does not include place of birth, date of birth, national identity number, nationality, civil status, profession, home address and place of work, unless such information reveals a client relationship or other matters that should be considered personal. Moreover, the King may prescribe further regulations concerning which information is to be considered personal, which agencies may disclose to private individuals such information as stated in the preceding sentence and other information concerning an individual's personal status, as well as terms and conditions for providing such information. The duty of confidentiality shall continue to apply after the person concerned has terminated their service or work. Nor may they exploit such information as is mentioned in this section in the course of their own business activities or in service or work for others.

Act of 20 May 2005 no. 28 (General Civil Penal Code)
Section 209 – Breaches of confidentiality
Any person who discloses information deemed by the law to be confidential or who uses such information to obtain for themselves or another person an unlawful gain shall be liable to a fine or a term of imprisonment not exceeding one year.

The first paragraph similarly applies to breaches of confidentiality arising from a valid instruction pertaining to services and work rendered for a government or municipal agency. The first and second paragraphs shall continue to apply to any person working for or rendering services to a government or municipal agency after the service or work has been completed.

Breaches resulting from gross negligence shall be punishable in the same way.

Aiding and abetting is not a criminal offence.

Section 210 – Gross breaches of confidentiality
Gross breaches of confidentiality are punishable by a term of imprisonment not exceeding three years.

When determining whether the breach is gross, particular emphasis shall be placed on whether the perpetrator intentionally sought to make an unlawful gain and whether the act has resulted in losses or a risk of losses for someone.

HELSE VEST IKT

Security instructions

Objective
The General Data Protection Regulation and health legislation impose strict rules on the processing of personal data. This is primarily based on the enterprise's duty to protect the availability and integrity of data in order to be able to provide vital healthcare. We must protect all the personal data that we process. Anyone making use of the services provided by the enterprise must also be able to feel reassured that their health and personal data is treated in confidence and protected against access by unauthorised personnel.

Scope and target group
All employees must comply with these instructions. The ICT security instructions apply to all staff, temporary staff, students, suppliers, consultants and others who are granted access to the company's information systems (referred to as users in the instructions). The stipulations contained in these instructions are minimum requirements that must be observed by everyone in order to ensure that laws are not breached. The ICT security instructions are a concise extract from the management system for data security and privacy that applies to the enterprise.

Any person to whom these instructions apply is personally responsible for familiarising themselves with and observing the instructions. In the learning portal you will find an e-learning course on data security. The course is mandatory for Helse XX HF employees and must have been passed before taking up employment and repeated at least every three years. The ICT security instructions and their provisions are part of the terms and conditions that you have agreed to.

Responsibilities

Design/maintenance of the procedure:	Committee for regional ICT security
Execution:	The general manager decides on and signs the ICT security instructions
Compliance:	All users of the ICT systems

A breach of the procedures and provisions contained in the ICT security instructions constitutes a breach of your obligations to the enterprise. A breach may therefore have consequences for your employment or contractual relationship with the enterprise.

Security rules

General diligence requirement
The fact that you, by virtue of your employment or contractual relationship with the health trust, are permitted to use the company's information systems carries a particular obligation to act ethically and with due diligence. You must therefore take a reflected approach to the sharing and storage of data. You must also be conscious of which searches and downloads you perform.

You must also be diligent in relation to what is communicated externally, on the internet via social media. You should therefore bear in mind that you are never anonymous online and that all online communication can be traced back to the computer you are using.

Observing confidentiality – access to documents
As a user of the enterprise's information systems you are obliged to actively prevent unauthorised parties from obtaining access to documents or other media that contain confidential personal data. A breach of the duty of confidentiality may have consequences for your employment and/or result in criminal liability.

Health data
It is unlawful to read, search for or in any other way obtain, use or possess confidential data unless it can be justified by the provision of healthcare to the patient, the administration of such care or if another act or regulation expressly permits it, cf. Section 21 a of the Health Personnel Act and Section 16 of the Personal Health Data Filing System Act.

Diligence to prevent access by third/unauthorised parties
Measures must be taken when processing health and personal data to prevent access by persons with no work-related need to view the data being processed.

Using the enterprise's information systems

Ownership and responsibility
The information systems and all associated equipment, software and stored data, with the exception of private data, are the enterprise's property and responsibility.

In given circumstances and subject to certain conditions the employer may be entitled to access documents and emails belonging to individuals. The conditions under which such access can be gained are regulated specifically in separate instructions in the security management system.

ICT equipment and software

Only ICT equipment, storage media and software acquired by the enterprise may be used on the company's network.

Employees who terminate their employment or take leave must return all assigned ICT equipment (computer, mobile phone, fob/card for remote access etc.) and software licences to the enterprise unless otherwise agreed.

Private use of the information systems

In principle the company's information systems must only be used for job-related tasks. However, limited use of the information systems for private purposes is permitted subject to the same prevailing rules.

A moderate number of private documents and emails may be stored in the information systems. They should be stored in a directory labelled "private".

Logging on and off, usernames, passwords and locking the workstation

- The password (and any fob/card for remote access) is the user's key to the enterprise's IT system and must not be disclosed or lent to others or left in the computer. This is the employee's personal responsibility.
- Using someone else's access details is not permitted.
- Passwords should not be written down. Any written down passwords must always be locked away or similar.
- The password should comprise at least 8 characters and must not be easily associated with the user.
- If there is any suspicion that a password has been obtained by others, it must be changed.
- A password-protected screen saver (Ctrl+Alt+Del) must be used when leaving the workplace/computer.
- Users must always log out of their user account before giving a computer to others. If the user has logged in as a "shared user", they must log out of all programmes and lock the screen.
- "Shared user" accounts must only be used for authorised purposes.
- Students should not use their student accounts when carrying out work as employees / temporary employees of the health trust.

Storage

- Health and personal data (incl. anonymised personal data) must not be stored in shared directories, portable storage media or the user's home directory without adequate access control. What constitutes adequate access control must be cleared with the ICT security manager.
- Solutions that cannot guarantee that the data is being securely stored in a defined location are not permitted. Storage outside the enterprise's control, including cloud storage, is deemed to be unsecure and must not be used unless its use has been risk-assessed and explicitly authorised.
- Quality assurance data and research data must be stored in dedicated directories. See the research procedures or contact the data protection officer for further information.

Data transfer

- Sensitive personal data must not be sent by ordinary email, fax, SMS or similar means without approved security arrangements. Nor is it permitted to send 11-digit national identity numbers in this way.
- Documents and storage media containing personal data must always be appropriately protected and sent using a sealed envelope/packaging.
- The sender is always responsible for ensuring that the recipient is authorised to receive the personal data in question and has been authenticated at the necessary level.

Document handling

- Printouts must be printed to the correct printer and collected immediately unless secure printing is used.
- Printouts containing personal data must be destroyed once the purpose of the printout has been achieved.
- Case documents must be archived in line with prevailing rules.
- Users who terminate their employment must clear their own file locations, emails, mobile phone and other electronic equipment and ensure that all information relevant to the enterprise is stored in the relevant directories. All other information must be deleted. Helse Vest ICT will delete any remaining information stored in a user's locations when the user's employment comes to an end.

Disposal/handling of equipment and storage media

- Hard disks, memory sticks and other equipment containing hard disks and other electronic storage media (such as tablets and smartphones) must be submitted to authorised personnel for appropriate destruction.
- Users who finish their employment must dispose of / handle all storage media in line with the enterprise's procedures.

Internet

The internet should be used with caution and in accordance with the enterprise's general ethical standards. Job-related tasks and functions along with information processed by the enterprise must not be compromised. Internet activities can be traced back to the enterprise and to the computer / user code from which the enquiry was made.

- It is not permitted to download and/or store files (programmes, graphics, audio, video etc.) on the enterprise's information systems unless it forms part of a work-related activity. Such downloads must be cleared with authorised personnel.
- It is not permitted to use online meeting places (screen, file, audio/image sharing) not offered by the enterprise.

Email and virus control

- Certain categories of personal data[1] must never be sent by unencrypted email.
- A distinction should be made between internal and external email. Labelling the start of the subject field with *"Ikke Sensitiv (IS:)"* [Non-sensitive] confirms that the information being transferred does not contain data that should not leave the enterprise. External emails not containing this labelling will be blocked by the security system.
- Internal emails should not be marked "IS:".
- Personal user codes must not be revealed in external email addresses.
- Any mass distribution of information must be job-related, and the person in charge of the distribution must take a critical view of the information and of its recipients.
- Generally speaking, emails should only be sent to recipients who require the information in question.
- Private email addresses and addresses belonging to other enterprises must not be used when carrying out activities on behalf of Helse Vest IKT.
- Due care should be taken when receiving emails. Attachments may contain viruses. If in doubt, contact the sender or the operational unit or delete the email.
- Email recipients should notify the sender if it is obvious that the recipient is not the intended addressee. Such emails must be deleted.

Outlook calendar

Many users have a shared calendar. This means that information entered in the meeting calendar is made available to the entire health trust and other Helse Vest enterprises.

- The meeting calendar must not contain particular categories of personal data, e.g. appointment diaries for named patients.
- Be cautious about what you write in meeting requests.
- Be cautious when sending documents as attachments to meeting requests. A meeting request can be made available only to meeting participants by ticking "Private".

Social media

You are responsible for observing the duty of confidentiality and protecting the integrity of patients and staff when using social media. Each enterprise has drawn up guidelines for such use. Note that social media can also be exposed to viruses.

Identifying and exploiting system weaknesses

Unless approval has been obtained, it is not permitted to identify or test potential system weaknesses, to attempt to access internal or external systems, to attempt to bypass established security mechanisms, to acquire extended access rights on local computers or to exploit any security weaknesses.

Security breaches

Suspicious activity and observed security breaches must be reported as non-conformities to your line manager and/or the ICT security manager as soon as possible. Any incident relating to a failure to observe these ICT security instructions will be considered a breach of security. A breach of the ICT security instructions will be considered a breach of the employment contract and the company's security management system and will be treated as an employment issue. Serious breaches of the security instructions will have consequences for the user's employment and may result in penal sanctions.

If you discover that information has gone astray or suspect that someone has been prying into your or other people's personal data, you must report it to your line manager and/or the security manager. It is better to raise the alarm once too often than once too little. Security non-conformities should be reported in the non-conformance system.

When reporting a non-conformity you can contact the ICT security manager, data protection officer, an employee representative or health and safety officer and request that your identity is not disclosed to the rest of the enterprise.

[1] Certain categories of personal data means: racial or ethnic origin, political views, religion, beliefs and union membership as well as the processing of genetic and biometric data with a view to conclusively identifying a physical person, health data or information about a person's sexual relationships or sexual orientation.

Loss or theft of equipment

Any loss or theft of equipment owned by Helse Vest enterprises or operated by Helse Vest ICT must be reported to the Helse Vest ICT customer service centre (+47 55 97 65 40 – 24 hrs) and your line manager. It is important that you report it immediately so that measures can be taken.