HELSE VEST IKT

# Non-disclosure agreement

**Background**
Confidentiality within the health service protects private interests and is rooted in the desire to protect individuals' personal circumstances and private sphere. Confidentiality is a key element of data protection. Another reason for observing confidentiality is so that patients can receive treatment. If healthcare staff and others were not bound to observe confidentiality, it could cause patients or their next of kin not to seek help for fear of information being passed on.

**Scope**
The duty of confidentiality applies to information that the signatory becomes party to in his/her work concerning people's 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 requires confidentiality for other reasons.

The duty of confidentiality also applies after the service or work has been completed.

**Statutory obligations**
The following describes a statutory duty of confidentiality (extracts from relevant legislation are given on pages 3-5 of this agreement[*]):

- under the Health Personnel Act section 21 health personnel are obliged to prevent others from obtaining information about people's health or medical conditions or other personal circumstances that they become party to in their capacity of health personnel. Nor may such information be read, sought or possessed except if the provision or administration of healthcare requires it or if another legal authority permits it.
- under the Specialist Health Service Act section 6-1 anyone providing services for health institutions affected by the act has a duty to observe confidentiality pursuant to the Public Administration Act section 13.
- under the Personal Health Data Filing System Act section 15 anyone processing health data under the Personal Health Data Filing System Act has a duty to observe confidentiality pursuant to the Public Administration Act section 13 and the confidentiality clauses in the Health Personnel Act.
- under the Patients' Rights Act section 3-6 information about health and medical conditions and other personal data must be treated in accordance with relevant legislation on confidentiality.
- under the Public Administration Act section 13 anyone providing services for a public agency is obliged to prevent others from obtaining information about personal circumstances and about technical equipment, methods and competition-related business matters that he/she may become party to during the course of the service.
- under the Personal Data Regulations section 2-9 staff shall observe confidentiality in respect of personal data where confidentiality is required. Steps shall be taken to prevent unauthorised access to both personal data and to data that is of significance to data security, cf. section 2-11.

**Breach of confidentiality**
Under the Health Personnel Act section 67 a breach of the provisions of the act is a punishable offence, including breaches of its confidentiality clauses.

Under the General Civil Penal Code section 121 it is a punishable offence to breach confidentiality imposed in pursuance of legislation or relevant instructions.

Under the General Civil Penal Code section 144 it is a punishable offence for medical practitioners, psychologists, chemists, midwives and nurses to reveal secrets confided to them in their course of duty.

Helse Vest IKT 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.

[*] All extracts are taken from www.lovdata.no and www.regjeringen.no with the exception of section 21a and parts of sections 25 and 45 of the Health Personnel Act, all extracts from the Specialist Health Service Act and section 13a of the Personal Health Data Filing System Act, of which no official or unofficial English translation appears to have been published.

**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 constitute 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 both Helse Vest IKT and the health trusts.

| Date of birth | Signature | Name in block capitals |
|---|---|---|
| | | |
| | Department, if employee of Helse Vest IKT / Company if external supplier/contractor: | |

# 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*

Health personnel shall prevent others from gaining access to or knowledge of information relating to people's health or medical condition or other personal information that they get to know in their capacity as health personnel.

*Section 21a – Prohibition of 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 – 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 responsible health care. The Personal Health Data Filing System Act section 13, third and fourth paragraphs, applies to electronic access to health data across enterprises.

The duty of confidentiality pursuant to section 21 is furthermore not to prevent personnel who are providing assistance with electronic processing of such information, or who is 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.

Personnel as mentioned in the first and second paragraph are subject to the same duty of confidentiality as health personnel.

*Section 26 – Information to the management of a facility and to administrative systems*

The health care provider may give information to the management of a facility when this is necessary in order to provide health care, or for the purposes of internal control or for the purposes of quality assurance of the service. The information shall in as far as possible be given without identifying characteristics.

The health care provider shall not be prevented by the duty of confidentiality pursuant to section 21 from providing the patient administration of the relevant facility with the patient's birth registration number, information relating to diagnosis, possible needs for assistance, offer of services provided, admittance and release dates as well as relevant administrative data.

The provisions relating to the duty of confidentiality shall apply correspondingly for personnel employed in patient administration.

*Section 45 – Transfer and release of and access to patient records and information therein*

Unless the patient objects thereto, health personnel as mentioned in section 39 may give the patient record or information therein to others who provide health care pursuant to this Act when this is necessary in order to provide health care in a responsible manner. The Personal Health Data Filing System Act section 13, third and fourth paragraphs, shall apply to electronic access to health data across enterprises. It shall be evident from the patient record that other health personnel have been given access to the patient records.

Health data mentioned in the first paragraph may be provided by the data controller in charge of the data or by the health personnel that have 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 health personnel may be given access to patient records, also in cases not included under 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 by fines 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.

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

*Section 6-1 – Confidentiality*

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

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

Information may only be provided to other public agencies under the Public Administration Act section 13 b, nos. 5 and 6, 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 18 May 2001 no. 24, Act on personal health data filing systems and the processing of personal health data (Personal Health Data Filing System Act)**

*Section 13a – Prohibition of unlawful appropriation of confidential information*

It is illegal to read, search for or in any other way obtain, use or possess health data processed under this act 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 15 – Duty of secrecy*

Any person who processes personal health data pursuant to this Act has a duty of secrecy pursuant to sections 13 to 13 e of the Public Administration Act and the Health Care Personnel Act.

The duty of secrecy pursuant to the first paragraph also applies to the patient's place of birth, date of birth, personal identity number, pseudonym, nationality, civil status, occupation, residence and place of work.

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 to facilitate the fulfilment of tasks pursuant to this Act, or to prevent significant danger to life or serious injury to a person's health.

**Act of 2 June 1999 no. 63 relating to Patients' 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 current 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 ceases to apply to the extent that the person entitled to confidentiality so consents.

If health personnel disclose information that is subject to a statutory duty of disclosure, the person whom the information concerns shall, insofar as is warranted by the circumstances, be informed that the information has been given and the nature of the 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 secrecy*

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 him in the course of his duties concerning:

1) an individual's personal affairs, or
2) technical devices and procedures, as well as operational or business matters which for competition reasons it is important to keep secret in the interests of the person whom the information concerns.

The term "personal affairs" shall not include place of birth, date of birth, national registration number, nationality, marital status, occupation or place of residence or employment, unless such information discloses a client relationship or other matters that must be considered personal. Moreover, the King may prescribe further regulations concerning what kind of information is to be considered personal, which agencies may give private individuals such information as stated in the preceding sentence and other information concerning an individual's personal status, as well as prescribing the terms and conditions for providing such information.

The duty of secrecy shall continue to apply after the person concerned has terminated his service or work. Nor may he exploit such information as is mentioned in this section in his own business activities or in service or work for others.

**Regulation 15 December 2000 no. 1265, Regulations on the processing of personal data (Personal Data Regulations)**

*Section 2-9 – Duty of confidentiality*

Members of the staff of the data controller shall be subject to a duty of confidentiality as regards personal data where confidentiality is necessary. The duty of confidentiality shall also apply to other data of significance for data security.

*Section 2-11 – Protection of confidentiality*

Measures shall be taken to prevent unauthorized access to personal data where confidentiality is necessary. The security measures shall also prevent unauthorized access to other data of significance for data security.

Personal data that are transferred electronically by means of a transfer medium that is beyond the physical control of the data controller shall be encrypted or protected in another way when confidentiality is necessary.

As regards storage media that contain personal data where confidentiality is necessary, the need to protect confidentiality shall be shown by means of marking or in another way.

If the storage medium is no longer used for the processing of such data, the data shall be erased from the medium.

**Act of 22 May 1902 no. 10, the General Civil Penal Code**

*Section 121*

Any person who wilfully or through gross negligence violates a duty of secrecy which in accordance with any statutory provision or valid directive is a consequence of his service or work for any state or municipal body shall be liable to fines or imprisonment for a term not exceeding six months.

If he commits such breach of duty for the purpose of acquiring for himself or another person an unlawful gain or if for such

purpose he in any other way uses information that is subject to a duty of secrecy, he shall be liable to imprisonment for a term not exceeding three years. The same applies when there are other especially aggravating circumstances.

This provision also applies to any breach of the duty of secrecy committed after the person concerned has concluded his service or work.

*Section 144*

Clergymen of the Church of Norway, priests or pastors in registered religious communities, lawyers, defence counsel in criminal cases, conciliators in matrimonial cases, medical practitioners, psychologists, chemists, midwives and nurses, as well as their subordinates or assistants, who unlawfully reveal secrets confided to them or their superiors in the course of duty, shall be liable to fines or imprisonment for a term not exceeding six months.

# Security instructions

**Introduction**

**To whom do the security instructions apply?**
These security instructions apply to all staff, temporary staff, suppliers, consultants and others who are granted access to the trust's electronic services.

**Background**
Health legislation in combination with the Personal Data Act sets out strict requirements for the processing of health and personal
data. Firstly, this is based on the health trust's duty to protect the availability and integrity of data in order to be able to provide vital healthcare. In addition, anyone making use of the services provided by the health trust must be able to feel reassured that his/her health and personal data is treated in confidence and protected against access by unauthorised personnel.

The stipulations contained in these instructions are minimum requirements that must be observed by everyone to whom the instructions apply, in order to ensure that laws are not breached.

**Responsibility**
Any person to whom these instructions apply is personally responsible for familiarising themselves with and observing the instructions. The instructions and their provisions form part of the terms and conditions that you have agreed to as an employee / temporary employee of the health trust. This also applies to those providing services to the health trust on the basis of the contractual obligations to which they have committed themselves.

A breach of the procedures and provisions contained in these instructions is a breach of your obligations towards the health trust whether you are an employee / temporary employee or a service provider. A breach may therefore have consequences with regard to employment or to the contractual relationship with the health trust.

**General diligence requirement**
The fact that you, by virtue of your employment or contractual relationship with the health trust, are permitted to use the trust's information system carries a particular obligation to act ethically and with due diligence. Individual users must therefore be actively aware of which searches and downloads of materials they perform.

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

**Security rules**

**Observing confidentiality – access to documents**
As a user of the health trust's information system you are obliged to actively prevent unauthorised parties from obtaining access to documents or other media that contain confidential data.

**Using the trust's information systems**

*Ownership and responsibility*
The information system and all associated equipment, software and stored data (including data about clients), with the exception of private data, are the trust's property and responsibility.

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

*Logging*
Internet and network traffic is logged in order to monitor the trust's security rules. This means that employees' online

activities and their use of programmes and services are recorded and that it is possible to trace these back if a breach of the trust's security rules is detected.

Logs from patient journals are reviewed regularly and in the event of suspected unlawful use by authorised personnel, as described in the trust's guidelines on such matters.

*Private use of the information system*

In principle the trust's information system must only be used for job-related tasks. However, the health trust does permit limited use of the information system for private purposes. These include:

- Word processing, calculations, sending and receiving emails, and viewing web pages provided their content is not unlawful.

A moderate number of private documents and emails may be stored in the information system. They should be stored in a location marked "private". Private emails that are not stored in a location that is especially marked for such purposes do not enjoy the same level of protection against access by the employer as if they were marked.

*ICT equipment*

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

- The installation of any equipment and software must be carried out by authorised personnel.
- The use of software other than the standard software provided by the trust must be approved by authorised personnel.
- Personal equipment must not be connected to the trust's network. This includes private USB storage devices, PDAs, mobile telephones, cameras and similar.
- External consultants and temporary staff must not connect their own computers to the trust's network but should use the guest network or be issued with a computer by the trust. Any special requirements for connecting own equipment must be cleared with authorised personnel.
- Equipment that does not form part of a mobile solution must not be connected to networks other than those provided in the workplace.
- Connecting to external networks, connecting with a modem/ISDN and/or sharing wireless networks while the computer is connected to the internal network are not permitted.
- Computer screens should be positioned to prevent access by unauthorised parties.

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

*Logging on and off, usernames, passwords and screensavers*

- The password (and any fob/card for remote access) is the employee's key to the trust's IT system and must not be revealed 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.
- Passwords must not contain names of family members, national identity numbers or other information that can be easily associated with the user.
- If there is any suspicion that a password has been obtained by others, it must be changed.
- Password-protected screensavers (Ctrl+Alt+Del) must be used and/or the door to the office must be locked when leaving the workplace/computer.
- Users must *always* log off from the network before giving a computer to others. If the user has logged in as a "shared user", he/she 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 trust.

*Data processing*

The Personal Data Act addresses data protection and sets out requirements for the protection of personal and health data. It applies from the moment basic information about an individual is recorded.

- A personal data filing system is in existence if personal details other than year of birth and initials are recorded. A register must have been granted a licence or notice of it given before it can be established. The need for a filing system, along with the need for technical protection, shall be assessed by the data protection officer (if it concerns research) or other authorised IT security personnel (ICT security manager and Helse Vest ICT if appropriate).
- Generally speaking, consent shall be obtained from the affected parties for all other use of sensitive personal data and personal data filing systems other than direct healthcare and statutory notification.
- Personal and health data held by the trust shall not be made available to unauthorised personnel or other unauthorised parties, including own staff.
- Employees are not permitted to search for patient data or other information that they do not require in their day to day work.
- It must be checked that printouts are made using the correct printer.
- Printouts must be collected immediately.

*Storage*

- Sensitive personal data must not be stored in shared locations (F:) or in the user's home location (H:) without adequate access protection. What constitutes adequate protection must be cleared with the ICT security manager.
- Sensitive personal data must not be stored on portable storage media (including the C drive on desktop computers) without adequate protection.

*Sending*

- Sensitive personal data must not be sent via ordinary email, fax or similar means without approved security arrangements.
- Documents and storage media containing sensitive 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 sensitive data in question.

*Destroying/deleting documents*

- Documents containing personal and health data must be destroyed when they are being disposed of.
- Employees who finish their employment must clear their own file locations and email and ensure that all information relevant to the trust is stored in relevant catalogues. Helse Vest ICT will delete any remaining information stored in a user's locations when that user's employment comes to an end.
- Employees who finish their employment must destroy or hand over their own documents in line with the above procedures.

*Disposal/handling of equipment and storage media*

- Hard disks, memory sticks or equipment containing hard disks and other electronic storage media must be submitted to *Miljøhallen* for appropriate destruction.
- Employees who finish their employment must dispose of / handle all storage media in line with the above procedures.

*Internet*

The internet should be used with caution and in accordance with the trust's general ethical standards. Work-related tasks and functions along with information processed by the trust must not be compromised. Internet activities can be traced back to the trust
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) to/in the trust's information system unless it forms part of a work-related activity.

*Email and virus control*

- A distinction should be made between internal and external email. The letters IS (meaning *Ikke Sensitiv* – non-sensitive) at the beginning of the subject field confirms that the information being sent does not contain sensitive personal data. External email not containing the letters IS will be blocked by the security system. Internal email should not be marked with the letters IS.
- National identity numbers must not be sent via email.
- 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.
- Due care should be taken when receiving emails. Attachments may contain viruses. If in doubt, contact the sender or the operative 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 meeting calendar*

Many employees use a shared meeting calendar. This means that information entered in the meeting calendar is made available to the entire trust.

- The meeting calendar should not be used for sensitive health and personal data, e.g. as an appointment calendar for patients.
- Be cautious about what you write in meeting requests.
- Be cautious when sending documents as attachments to meeting invitations. A meeting request can be made available only to meeting participants by ticking "Private".

*Mapping and exploiting system weaknesses*

It is not permitted to map 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 incidents and observed security breaches must be reported to the line manager and/or ICT security manager. Any incident relating to a failure to observe these security instructions will be considered a breach of security. A breach of the security instructions will be considered a breach of the employment contract and the trust's ICT security management system and will be treated as an employment issue. A serious breach of the provisions in the security instructions will have consequences for the person's employment and may result in legal action being taken.