Code of conduct for information security
www.normen.no

Published with the support of:

Direktoratet for e-helse

Access control

Supporting document
Fact sheet no 14
Version: 4.0
Date: 4 June 2015

Purpose	The purpose of access control is to ensure that health and personal data only are available in accordance with official needs. This entails: • That users are authenticated in a satisfactory manner. • That access is granted, administered, controlled, and removed.		
Responsibility	The data controller is responsible for access being managed in such a manner that access is only granted in circumstances where there is an official need. Individual employees are bound by a duty of secrecy concerning health and personal data. For research projects, the project manager must ensure that access control has been implemented.		
Execution	Access control must be subject to continuous supervision.		
Scope	All organizations in the healthcare, care, and social services sector must ensure that access to health and personal data is only granted to the extent that it is needed for an individual's tasks, and in compliance with the current provisions concerning the duty of secrecy.		
Target group This fact sheet is particularly relevant for:	☒ Organization manager/ management ☐ Person/body responsible for research ☒ Project manager – research ☒ Head of security/Security coordinator	☐ Staff/employee ☐ Researcher ☐ Privacy protection ombudsman	☒ ICT manager ☒ Data processor ☒ Supplier
Authority	Access to personal health data is governed by, amongst other things: • The Public Administration Act section 13 • The Health Personnel Act section 21 • The Health Personnel Act section 25 • The Health Personnel Act section 45 • The Patient Records Act section 15 • The Patient Records Act section 16 • The Patient Records Act section 17 • The Patient Records Act section 19 • The Personal Health Data Filing System Act section 15 • The Health Research Act section 7 Other relevant provisions may be found in, amongst other things, the Personal Data Act, the Patients' and Users' Rights Act, the Regulations concerning interorganizational access to personal health data, and the Patient Records Regulations.		
References	• The Code of conduct for information security, Chapter 5.2 • Framework for Authentication and Non-Repudiation in Electronic Communication in and with the Public Sector, April 2008		

Patient information must be protected, but healthcare personnel providing medical assistance must be able to look up and register relevant and necessary information in the patient's record. This is taken of care of through, amongst other things, access control.

Access control depends on authentication and authorization. Authentication entails that the user must identify himself to the ICT solution by means of an authentication mechanism such as user name/password, smart card, or similar. Authentication shall ensure that the right person is authorized and gains access to health and personal data, and that incident registrations indicate the actual person

who has had access. The authentication mechanism must be of a sufficient quality and strength – and must be assigned in a satisfactory manner. Authorization entails the assignment, administration, and control of access to information contained in the ICT system. Access shall be on the basis of an official need.

Authentication
Authentication must be of sufficient strength relative to its purpose, and different uses entail different strength requirements:

- For login to internal systems (networks, internal EPR, etc.) user name/password should be the minimum requirement – the system should be configured to require a minimum of 7 characters, at least one number and both capital and lowercase letters.
- In the case of external login, be it from external networks or through interorganizational access, the authentication must satisfy the requirements specified in chap. 5.2.1 of the Code:
    - If portable equipment, a *home office*, and wireless communication are used, the *authentication* must not entail an increased risk in comparison to that applicable to the use of fixed equipment. A risk assessment must show that the authentication solution provides satisfactory security.
    - In the case of interorganizational *access* to *personal health data* a *secure authentication system* must be utilized.

Assignment of user identity and authentication mechanism must be done in a satisfactory manner by the organization, and should include appearing in person presenting proof of identity, unless the person assigning the user identity already knows the user.

Authorization
The organization shall establish a procedure for assigning, administering, and controlling rights of access. Access to health and personal data may only be granted when necessary for getting sufficient information to provide, or assist in the provision of, a medical procedure, with the patient's consent, or in accordance with statutory exemptions from the duty of secrecy.

If the organization has implemented procedures for principle of necessity access authorized users may be given the option to grant themselves access. The justification for *principle of necessity access* shall be documented and each separate incident shall be followed up as a *nonconformity*. If the patient's situation is so severe that it may be justified based on concerns for the patient's life and health principle of necessity access may also be used to access information subject to a reservation against access.

Roles
Clearly defined roles and role templates may be helpful in defining rights of access in an EPR system. Organizational roles alone will not be sufficient to grant access to health data. Organizational roles may determine the kinds of decisions related to the provision of medical treatment the persons assuming the role may take (and take part in the execution of), as well as in which parts of the organization they have the right to make such decisions. The roles should then be defined in accordance with the organizational structure and the information needs different groups of employees will have in a treatment situation – some examples may be:

- Consultant in the anaesthetic department
- Nurse in ward A7
- Consultant in the department of internal medicine

Role template examples:

- Consultant
- Nurse

The level of detail in defining different roles may depend on the size and structure of the organization.

Decision-based access control
Decision-based access control means that a decision to provide medical care to the patient in question must be present before access to the patient's record may be granted. This form of decision-based access control differs from the more traditional role-based access control in that it is the concrete involvement with the patient, and not organizational role of healthcare personnel, that determines whether access may be granted. The organizational role of healthcare personnel does, however, determine the kinds of decisions to provide medical treatment that an individual may make/participate in the execution of.

The decisions that form the basis for the granting of access must be recorded in the patient's record, but the standard condition (medical care) may be recorded automatically. If access is granted based on a need to provide emergency care or a request for patient access to records, this should be made explicit in the record.

Decisions to provide treatment, consent (or the opposite, the opportunity to refuse consent), as well as statutory exceptions to the duty of secrecy, are decisive in granting access to patient records. Access can only be granted when necessary to gain sufficient information to provide, or assist in the provision of, medical care or other statutory interventions. This may be done by making the information accessible during the period of time a patient is referred to a department for evaluation or treatment, or by authorized healthcare personnel making a decision to provide medical care to a patient. Healthcare personnel actively collaborating in the treatment of the patient in question may be granted access to looking up necessary information internally as long as the personnel in question are collaborating.

Example of access control for EPR in healthcare institutions (from the EPR standard):
Control of access to information contained in patient records in healthcare institutions may on this basis be based on the following core principles:

Creation of patient record	When a decision to provide medical care to a patient has been made a patient record must be created, unless such a record has already been created in connection with previous provision of medical care. Cf. the Patient Records Regulations section 5.
Individual responsible for the patient record	In healthcare institutions one person shall be designated as the person with a superior responsibility for the individual patient record, cf. the Health Personnel Act section 39 and the Patient Records Regulations section 6. In order to properly attend to his responsibilities the person with a superior responsibility for the individual patient record should in the main have access to the entire record.
Access for healthcare personnel	Healthcare personnel having responsibility for providing treatment or other medical care must be given access to necessary information contained in the patient record. Such access may be granted implicitly, e.g. as a consequence of a decision to admit the patient to hospital in order to provide a specific form of treatment being recorded in a patient's hospital record. Or, similarly, when it is recorded in the record kept by the nursing service that the patient has accepted an offer of admission to a nursing home.
Healthcare personnel's ability to record information	Healthcare personnel providing medical care to the patient must be given the ability to record relevant and necessary information concerning the medical care in the patient's record. Cf. the Health Personnel Act sections 39–40.

Roles and patient records access	The role filled by healthcare personnel determines the procedures concerning medical care an individual may decide is to be carried out and which procedures the individual may assist in the carrying out of. Such roles do not, however, in themselves grant access to patient records. Only after a decision has been taken that entails that the person filling a role becomes involved in the provision of medical care can access to necessary information in the patient record be granted.
Sharing of data with co-operating personnel	Certain decisions concerning procedures may entail that information from patient records must be provided to co-operating personnel, cf. the Health Personnel Act section 25 and the Patient Records Act section 19. When entering such a procedure in the record access to the information may automatically be granted to personnel co-operating in the execution of the procedure. This of course on the assumption that this does not conflict with the consent the patient has given to access to his record.
Access restricted to official need	No one shall be given access to more information contained in patient records than what is required to execute the tasks entailed by his role. When the need for access to patient record information has ended, e.g. because a procedure has ended, access shall be terminated.

Example of access control in small organizations (e.g. a GP surgery)
The following may be sufficient for EPR systems intended for the use of general practitioners:

Creation of patient record	When a new patient is received for treatment the general practitioner shall create a record for the patient. The general practitioner shall be responsible for keeping the record up to date and shall have access to the entirety of its contents.
Blocking of patient record	If the patient desires that no one but his regular general practitioner shall have access to the record, the record must be blocked, ensuring that no one else may access it.
Sharing of records with co-operating personnel	Unless the patient desires his record blocked, the general practitioner shall grant access to all or relevant parts of the record to co-operating personnel (medical secretary, other general practitioner working in the surgery, etc.). It must be possible, when needed, to time-limit such access. If the patient, in the absence of his regular general practitioner, wishes to receive treatment from another general practitioner at the surgery, this general practitioner may be given access to the patient record. Prior to such access the general practitioner must record the decision that forms the basis for unlocking the record.
Transfer of practice	If a general practitioner transfers his practice to another general practitioner, that individual should be able to be registered as the person with the superior responsibility for all patient records from a given date, taking over the original practitioner's rights as regards these records. This, however, does not apply to the records of patients that do not wish to be treated by the new practitioner. These must be handled as specified in the Patient Records Regulations section 15.

Similar basic systems may be developed by other kinds of smaller organizations.

Release of information internally in an organization in connection with patient care
The release of health data must be based on decisions made after concrete evaluation of need. When a decision to release information has been made there are several alternatives as to how to release the information. One alternative is electronic messages. Another alternative is that the information is made accessible to the person to whom it has been released.

Review and follow-up
Access to EPR shall be documented in the record, indicating the person who received access and the time and duration of the access.

The organization should have procedures for reviewing incident registers in order to uncover unauthorized access (cf. Fact sheet 15 – Incident registration and follow-up), as well as deactivating user accounts that are not in use.