Code of conduct for information security
www.normen.no

Published with the support of:

Helsedirektoratet

# Incident registration and follow-up

**Supporting document**
**Fact sheet no 15**
Version: 2.1
Date: 15 Dec 2010

| | |
|---|---|
| **Target group**<br>This fact sheet is particularly relevant for: | ☒ Supplier<br>☒ ICT manager<br>☐ Researcher<br>☒ Project manager<br>☒ Head of security/Securityy coordinator<br>☒ Organization manager/management<br>☐ Person or body responsible for research<br>☒ Staff/employee<br>☒ Data processor<br>☐ Privacy protection ombudsman |
| **Responsibility** | The data controller is responsible for incident registration, but daily tasks are normally delegated to the person responsible for the individual information system.<br>The project manager has a special responsibility in connection with research projects. |
| **Execution** | Planned prior to the use of a new information system, and executed while it is being used. |
| **Purpose** | The purpose of incident registration and follow-up of incident registers is to:<br>• provide an overview of authorized use of health and personal data in the organization<br>• enable the organization to uncover unauthorized use, or attempts at unauthorized use, of health and personal data<br>• prevent, uncover, and counter repeats of security breaches in the information systems<br>• facilitate the patient/user's right of access to incident registers, in order that he may be able to attend to his rights<br>• facilitate employees' right of access to information stored about them in the incident register |
| **Scope** | All sector organizations processing health and personal data electronically must keep and control incident registers |
| **Authority** | The Personal Data Regulations sections 2-14, 2-16, and 7-11. |
| **References** | • The Code of conduct for information security, Chapters 5.2, 5.3, 5.4, 5.5 and 5.7, 6.5, (www.normen.no)<br>• The Personal Health Data Filing System Act section 13a<br>• The Health Personnel Act section 21a.<br>• EPR standards: www.kith.no/templates/kith_WebPage____833.aspx<br>• Guidelines for remote access for maintenance and updates between supplier and health organization, (www.normen.no)<br>• Personal data protection and information security in research projects in the healthcare and care sector, (www.normen.no) (in Norwegian only)<br>• Fact sheet 47 – Register of authorizations |

The requirements found in this fact sheet will become legal requirements with the adoption of the Statutory Instrument 'Regulations concerning information security, access control, and access to personal health data in personal health data filing systems established for therapeutic purposes'.

| No | Action |
|---|---|
| 1. | **Incident registration procedure**<br>a) The data controller shall ensure that procedures are implemented that ensure that incident registration is implemented<br>b) The procedures shall<br>- take into consideration that incident registration may entail a new processing of personal data that may be subject to a duty of reporting. The reporting duty does not apply if the processing is for the purpose of<br>○ administering the system, or<br>○ uncover/clear up security breaches in the computer system<br>- attend to the requirement that it shall be possible to compare incident registers to the register of authorizations and the presence register |

| No | Action |
|---|---|
| | - attend to the requirement that incident registers be analysed in such a manner that incidents are detected before they may have any serious consequences, and preferably within 1 week<br>- attend to the requirement that the Data Inspectorate is to be notified if health and personal data have been disclosed or accessed without authorization |
| 2. | **Incident registration shall be implemented for**<br>a) Access to personal health data filing systems established for therapeutic purposes and specialized systems<br>- All access to personal health data filing systems established for therapeutic purposes and specialized systems<br>- All attempts at unauthorized use of personal health data filing systems established for therapeutic purposes and specialized systems<br>- All principle of necessity access with the reason for such access<br>b) Infrastructure<br>- Incidents relevant to security in security barrier (e.g. firewall and router), such as:<br>o All attempts at illegal access, both internal and external<br>o All violations of rules prohibiting traffic<br>o All violations of rules that allow legal traffic from external connections<br>- All attempts at unauthorized use of network operating systems |
| 3. | **Incident registration in research projects shall be implemented for**<br>a) All research access, registration, correction, and deletion, authorized and unauthorized attempts to use and copy/duplicate<br>- research data<br>- the research file<br>b) All authorized and unauthorized attempts to use and copy/duplicate<br>- the re-identification key<br>- file containing re-identification keys<br><br>Both manual and electronic incident registration may be utilized. |
| 4. | **The incident register must, at minimum, contain**<br>a) For authorized use:<br>- The unique identifier of the authorized user (see Fact sheet 47 – Register of authorizations)<br>- The role of the authorized user when accessing<br>- Organizational affiliation of the authorized user (usually organization or data processor)<br>- The internal organizational (departmental) affiliation of the authorized user (department name or department code is usually sufficient). May be the same as the organizational affiliation if the organization is not structured into separate departments<br>- The kind of information to which access has been granted<br>- The reason for access (e.g. medical care, principle of necessity access, administrative use)<br>- Time and duration of the access (date and time)<br>- The reason for the use of principle of necessity access<br>- For remote access from supplier:<br>o traffic initiated to IP address and port number<br>o which actions have been executed (commands, transactions, etc.). If possible the time of execution for any commands shall be noted in the incident register<br>o the data/data files that have been downloaded by the supplier (data files) or uploaded to the organization (program files and patches)<br>o Name and unique identifier of the person(s) having utilized the remote access in question<br>b) For attempts at unauthorized use:<br>- The user identity utilized<br>- Time (date and time) |

| No | Action |
|---|---|
| | IP address or other identification of PC/work station used (e.g. MAC address or NAT address) |
| 5. | **Incident register security and storage**<br>a) The incident registers shall be secured against access, editing, and deletion by unauthorized personnel<br>b) Incident registers must be stored for a minimum of 2 years |
| 6. | **The incident register as evidence**<br>a) An incident register that is to be used as evidence should be mirrored to a separate storage medium prior to analysis<br>b) The mirroring should take place under the supervision of 2 or more persons<br>c) A written record of the mirroring should be created, indicating the actions undertaken. The record must be signed by all persons present and stored together with the registered nonconformity |
| 7. | **Use of the incident register**<br>a) Electronic incident registers shall be easily analysed with analysis tools with a view to uncovering violations of the rules (see also the Personal Health Data Filing System Act section 13a and the Health Personnel Act section 21a.)<br>b) For manual incident registers the organization shall create procedures for satisfactory analysis of the registers<br>c) If violations are uncovered sanctions against employees must be imposed<br>d) If sanctions do not have the necessary effect, i.e. there is repeated access by several unauthorized persons, necessary technical measures must be implemented<br>e) All use of principle of necessity access must be documented and each incident must be followed up as a nonconformity in order to ensure that the reason for the use of such access was relevant<br>f) When rules concerning connection to a network outside the organization are violated, the channel must be closed until a new secure solution has been implemented<br>g) When rules concerning the logical separation of the Internet and a network in which health and personal data are being processed are violated the violation shall be handled as a nonconformity and employee sanctions considered<br>h) When rules forbidding the disclosure of sensitive personal data via e-mail are violated the violation shall be handled as a nonconformity and employee sanctions considered |
| 8. | **Deletion of incident registers**<br>a) If records in the incident register may be connected to an individual the incident register must be deleted when its security-related purposes have been fulfilled but only after the passage of 2 years |