
 <p>Code of conduct for information security www.normen.no</p>	<p>Published with the support of:</p> 
<h2>Register of authorizations</h2>	<p>Supporting document Fact sheet no 47 Version: 1.1 Date: 15 Dec 2010</p>

<p>Target group</p> <p>This fact sheet is particularly relevant for:</p>	<input checked="" type="checkbox"/> Supplier <input checked="" type="checkbox"/> ICT manager <input type="checkbox"/> Researcher <input checked="" type="checkbox"/> Project manager	<input checked="" type="checkbox"/> Head of security/Security coordinator <input checked="" type="checkbox"/> Organization manager/management <input type="checkbox"/> Person or body responsible for research	<input type="checkbox"/> Staff/employee <input type="checkbox"/> Data processor <input type="checkbox"/> Privacy protection ombudsman
Responsibility	The data controller is responsible for creating a register of authorizations of the necessary scope, and for stipulating procedures for the use of the register.		
Execution	When creating information systems which require authorizations for accessing health and personal data.		
Purpose	A register of authorizations shall detail the accesses and roles an individual has and has had. The register shall form the basis for reviewing access to health and personal data, and it shall be possible to compare it with other registers such as the incident registers.		
Scope	The register of authorizations shall contain all accesses and all roles for access to personal health data filing systems established for therapeutic purposes (including electronic patient records (EPR)) and specialized systems.		
Authority	No formal statutory authority		
References	<ul style="list-style-type: none"> Code of conduct for information security, Chapter 5.2.2. (www.normen.no) Fact sheet 15 – Incident registration and follow-up 		

“*Authorize/authorized/authorization*” means, for the purposes of the Code, that a person in a certain role may be granted or has been granted specific permissions to read, register, edit, correct, delete and/or block personal and health data. Authorization may only be provided insofar that it is necessary in order for an individual to fulfil his or her duties, is justified on the basis of an official need, and is in accordance with any and all provisions regarding the duty of secrecy.

No	Action
1.	<p>Background</p> <p>a) The organization shall always ensure that personnel have authorization for accessing health and personal data in connection with</p> <ul style="list-style-type: none"> – medical care or the administration of such care – responding to enquiries concerning personal health data and for other particular purposes – the work of the control commission within mental healthcare – social and care services
2.	<p>Requirement for a authorizations register</p> <p>a) The organization shall keep a register (register of authorizations) of all authorizations issued, cf. paragraph 1</p> <p>b) The register shall include information concerning:</p> <ul style="list-style-type: none"> – unique identifier of the authorized person (preferably not the personal identity number used directly) – the name of the authorized person – organization – organizational unit – the role the authorization has been issued for – the purpose of the authorization

No	Action
	<ul style="list-style-type: none"> - the time the authorization was issued - the time the authorization was/is valid from - the time, if any, the authorization was changed - time the change was valid from - time, if applicable, the authorization was recalled (e.g. because of resignation, leave of absence, etc.) <p>c) The register should include:</p> <ul style="list-style-type: none"> - the name and unique identifier of the person registering the issued/changed authorization <p>d) The register may be kept manually or electronically. An electronic register is recommended</p>
3.	<p>Comparing the register of authorizations with the incident register</p> <p>a) The organization shall establish a procedure for such comparison</p> <p>b) The comparison need not be done electronically</p> <p>c) The organization may compare the register of authorizations with incident registers when</p> <ul style="list-style-type: none"> - Inspection related to a justifiable suspicion of unauthorized access (cf. the Health Personnel Act section 21a and the Personal Health Data Filing System Act section 13a) - The patient's right of access to incident registers - System administration <p>d) The comparison shall result in the user identity in the incident register</p> <ul style="list-style-type: none"> - being connected to the correct person - showing the role the user had at the time of registration
4.	<p>Storing the register of authorizations</p> <p>a) Entries in the register of authorizations may deleted 5 years subsequent to the latest use of the authorization</p>