Norm for informasjonssikkerhet
www.normen.no

Published with the support of:

Helsedirektoratet

Damage limitation when data have been disclosed accidentally

Supporting document
Fact sheet no 41
Version: 2.1
Date: 15 Dec 2010

Target group This fact sheet is particularly relevant for:	☐ Supplier ☒ ICT manager ☒ Researcher ☒ Project manager	☒ Head of security/Security coordinator ☒ Organization manager/management ☒ Person or body responsible for research	☒ Staff/employee ☒ Data processor ☐ Privacy protection ombudsman
Responsibility	The organization's manager is responsible for the correct handling of the accidental disclosure of health and personal data.		
Execution	The organization must establish procedures for handling the accidental disclosure of health and personal data. The fact sheet may form the basis for such procedures.		
Purpose	The correct handling of the accidental disclosure of health and personal data as well as providing employees with training in the handling of accidental disclosure.		
Scope	All accidental disclosure of health and personal data		
Authority	The Personal Data Regulations section 2-6		
References	• The Personal Health Data Filing System Act section 33 • The Personal Health Data Filing System Act section 34 • The Personal Health Data Filing System Act section 35 • Personal data gone astray (22 Nov 2007), the Data Inspectorate, An action plan for organizations: http://www.datatilsynet.no/templates/article____2071.aspx • Fact sheet 7 – Risk assessment • Fact sheet 8 – Handling nonconformities • Fact sheet 15 – Incident registration and follow-up • Fact sheet 17 – The physical security of areas and equipment • Fact sheet 19 – Measures to obstruct malignant applications • Fact sheet 22 – Control and security of external access • Fact sheet 30 – Portable equipment • Fact sheet 34 – The handling of storage media • Fact sheet 36 – Remote access for maintenance and updates • Fact sheet 42 – Use of SMS for patient contact		

Accidental disclosure refers to incidents that have caused the accidental disclosure of health and personal data.

No	Action
1.	**Stop and limit the disclosure of health and personal data** a) Report the incident internally b) Place responsibility on one person who will lead and organize damage limitation c) Survey and document the main elements of what has happened. Use established procedures and forms for handling nonconformities d) Implement necessary immediate measures for ending and limiting the disclosure: - if health and personal data have been disclosed through an error, request their destruction - if health and personal data have been published due to an error, request their deletion - immediate technical measures to restore the secure solution. The technical solution is particularly vulnerable in relation to updates that change the configuration and setup of security barriers - physical measures to limit access to health and personal data - administrative measures e) When necessary secure evidence without removing or damaging stored data. Contacting experts at securing data evidence may be necessary

No	Action
	f) Evaluate whether it is necessary to contact the police. This depends on what has happened, and how it happened. The data controller determines whether this should be done
2.	**Document the type and scope of health and personal data disclosed** a) Describe the type and scope of health and personal data disclosed. May the data be used (are they encrypted or not)? b) Document the sequence of events and the cause of the disclosure. The reasons may be technical, physical, or administrative. Make use of incident registration, when relevant, for a detailed survey of the incident. Examples of the accidental disclosure may include - Accidents, such as printouts of patient records being mislaid, the loss of a portable computer on which health and personal data are stored, or storage media being sent via registered post going astray - Intentional acts such as voyeuristic access or printout of electronic records (of famous persons) for whom one is not health personnel providing medical care, or the sending of health information via e-mail - Criminal acts such as theft of the central server containing the electronic patient records system from the general practitioners' surgery, theft of work stations and portable equipment, and tapping of the wireless network - System errors (functional or configuration errors) leading to printouts being sent to the wrong printer, a user gaining access to electronic patient records belonging to a different organization when making use of an external operations supplier (data processor), laboratory messages being sent to the wrong recipient, other messages being sent to the wrong recipient to/from the organization c) Describe who have been affected by the incident. E.g.: - Patient(s) - Health personnel - Next of kin/parents or guardians - The organization - Supplier - Staff d) Describe the damages resulting from the incident, e.g.: - Exposure of personal health data - Loss of personal health data - Media attention - Lawsuit against the organization or affected parties - Is this a repeat or one-off incident
3.	**Reporting the incident** a) In cases where the police are involved all reporting must be clarified with the police b) Notify all affected parties in accordance with paragraph 2c above. The data controller must consider which affected parties shall be notified and which considerations should be emphasized in the notification itself. When affected parties are notified they may themselves contribute to the damage limitation and in preventing further damage. The means and content of the notification should be proportionate to the incident and the information disclosed. The more serious the disclosure is for the individual, the more direct the notification should be c) Notify the Data Inspectorate in order to comply with the organization's duty to notify as specified in section 2-6 of the Personal Data Regulations. The notification will normally include - Complying with the duty to notify - Description of the incident - Description of the type and scope of information disclosed - The cause of the incident - Measures that have or will be implemented - Who have been notified of the incident - The organization's contact person for further information

No	Action
	d) Report internally who the affected parties are and how they have been notified e) Depending on the scope and type of accidental disclosure the incident may be become a matter for the media, something which may have an impact on both the organization and the affected parties. In such cases the organization must determine how to handle the media interest
4.	**Measures to rectify the damage** a) Determine how health and personal data have been disclosed (e.g. e-mail, memory sticks gone astray, failure in the technical solution, portable computer, website errors, printouts) b) Audit the security of existing measures and solutions that should have prevented the incident in order to uncover whether existing security solutions and procedures need to be changed and whether new measures need to be implemented c) Advise affected parties as to how they can or should act to limit the damage d) In cases where health and personal data has been released on the Internet, search engines, the National Library of Norway, Internet libraries in general and other Internet parties shall be contacted and directed to delete the information. This because several of these index and make copies of any publication e) The Data Inspectorate may advise on measures to rectify the damage
5.	**Prevent recurrence** a) Detailed review of the causes and survey whether this is an one-off incident or whether the disclosure may recur b) Perform risk assessment of new solutions in order to uncover any weaknesses c) Develop a plan of action d) Implement suggested measures in order to prevent recurrence e) Consider if an internal or external investigation of the incident is needed