
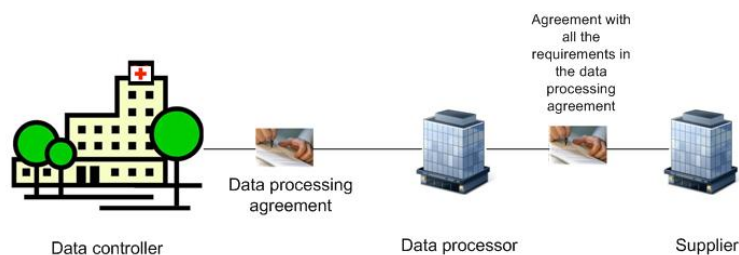
 Code of conduct for information security www.normen.no	Published with the support of: 
<h2>Use of data processor (external business unit)</h2>	Supporting document Fact sheet no 10 Version: 4.0 Date: 12 Feb 2015

Purpose	That health and personal data are not being processed by the data processor in a manner not agreed to by the data controller.		
Responsibility	The management of the data controller organization is responsible for drawing up a data processing agreement with the data processor (the external business unit). The data processor has an independent responsibility for ensuring that the processing of health and personal data is in compliance with the existing legal framework, as well as the Code, when this has been agreed.		
Execution	When health and personal data are being processed by an external business unit or when an external supplier is performing maintenance or updates requiring access to health and personal data.		
Scope	All organizations in the healthcare sector must enter into a data processing agreement when health and personal data are being processed externally. The scope of the data processing agreement must be adapted and limited to the processing of health and personal data that will be contracted out to the external business unit. Equivalent agreements must be made with external security suppliers that are implementing security measures.		
Target group This fact sheet is particularly relevant for:	<input checked="" type="checkbox"/> Organization manager/management <input checked="" type="checkbox"/> Person or body responsible for research <input checked="" type="checkbox"/> Project manager – research <input checked="" type="checkbox"/> Head of security/Security coordinator	<input type="checkbox"/> Staff/employee <input type="checkbox"/> Researcher <input checked="" type="checkbox"/> Privacy protection ombudsman	<input checked="" type="checkbox"/> ICT manager <input checked="" type="checkbox"/> Data processor <input checked="" type="checkbox"/> Supplier
Authority	<ul style="list-style-type: none"> • The Personal Data Act section 13 • The Personal Data Regulations section 2-15 		
References	<ul style="list-style-type: none"> • Code of conduct for information security, Chapter 5.8 • Fact sheet 15 – Incident registration and follow-up • Guidelines for remote access for maintenance and updates between supplier and health organization • Guidelines for personal data protection and information security in the healthcare and care sector • Guidelines for information security in connecting municipalities, county municipalities, and the health net 		

Background

As shown in the below figure the data controller must enter into a data processing agreement with the data processor (external business unit). Additionally, the data processor must ensure that the requirements detailed in the data processing agreement are reflected in its agreements with its suppliers. A data processor is an external person or organization independent from the data controller's organization. The data processor processes health and personal data on behalf of the data controller. This entails that if the organization's ICT systems (any or all) are being run by an external business unit, this external business unit is a data processor.



By *processing* is meant any purposeful use of health and personal data, be it, e.g., collection, recording, collocation, storage, and disclosure, or a combination of such uses. Other uses of health and personal data that require a data processing agreement include converting, modifying, linking to other registers, analysing, reporting, testing, disposing, and deleting such data. Thus, even if the data processor is merely storing the data a data processing agreement is required. The same applies, to take another example, if the data processor is only registering the information on the data controller's behalf. The same furthermore applies if storage of the data is required when servicing computing equipment.

A question that often arises is whether a data processing agreement is required if the external organization is storing encrypted data. The answer is yes, as encryption merely constitutes a security measure, and the external organization is thus still storing health and personal data.

Examples of data processors:

- EPR supplier in cases where the server is physically located at the supplier's premises, and where the data controller (in the organization) has access to the EPR system through a terminal server solution.
- A supplier with remote access who is responsible for operating the whole or parts of the EPR system or the security system
- One of the partners in a formalized working partnership is operating the EPR system on behalf of the other partners. This applies to already established formalized working partnerships as the regulations have been rescinded. The new legal authority for multi-organizational collaboration on personal health data filing systems for therapeutic purposes is section 9 of the Patient Records Act.
- A supplier of a pay and personnel system in cases where the server is physically located at the supplier's premises, the supplier then being responsible for the operation of the system on behalf of the customer. Please note that the Personal Data Act, not the Patient Records Act, then regulates the matter and that the data processing agreement needs to be changed to reflect this and other matters (see the example of a data processing agreement, below).
- A group of companies centralizes the operation of all EPR systems to a single company created for this purpose
- Municipalities that use a host municipality or create intermunicipal companies for the operation of health and personal data ICT systems, including the municipalities' connection to the Norwegian Health Net
- The organization/research project may need that an outside group, a subcontractor, process or operate data on behalf of the project
- A health trust outsources the ICT system for processing health and personal data to a business unit external to the trust
- Suppliers erasing the contents of storage units (multifunction printer, disks, etc.) that are being decommissioned
- Use of cloud services for the processing of personal health data. The organization must identify any use of subcontractors by the cloud services supplier in order to ensure that the requirements of the Code of Conduct are applied to all processing of health and personal data

No	Activity/Description
1	Decision to use an external business unit After the decision that ICT systems (some or all) should be operated by an external business unit, and prior to such systems actually being handed over to the external business unit, a data processing agreement must be drawn up.
2	Identifying external business unit If an external business unit is already being used without the existing agreement defining the requirements attendant to the processing of health and personal data, such an agreement must be amended to include such requirements. A register of all external business units processing health and personal data must be kept at all times.
3	Drawing up a data processing agreement The data processor has an independent responsibility for information security according to the Patient Records Act section 22, the Personal Data Act section 13, and the Personal Data Regulations section 2-15 <u>The following minimum requirements are applicable to a data processor, and must be made explicit in the agreement:</u>

No	Activity/Description
	<p>a) The data processor must satisfy the minimum requirements of the Code (see chap. 4.4 Acceptable risk level). In order to satisfy these requirements it is recommended, at a minimum, that the organization's security objectives and strategy are included with the agreement (for further details, see subsection 4)</p> <p>b) The data processor must not process health and personal data in a manner not agreed to by the data controller</p> <p>c) If a data processor processes health and personal data on behalf of several organizations the data processor must ensure, through technical measures that cannot be overridden by users, that:</p> <ul style="list-style-type: none"> - The organizations are separated in line with the risk assessment, both as concerns databases containing data and as concerns communication - No one but the data processor, those working under the authority of the data processor, and the organization itself have access to the information <p>The data processor must also, in relation to this, ensure that measures have been taken ensuring that the Code's requirements concerning the level of acceptable risk have been met.</p> <p>d) It is recommended that the data processing agreement is included as a part of the general agreement between the organization and the data processor. E.g. as a part of:</p> <ul style="list-style-type: none"> - The Service Level Agreement and/or Purchasing Agreement regarding operational services - Or as an attachment to the Service Level Agreement or Purchasing Agreement <p>e) The data processor must have implemented procedures for authorization and access control that ensure that access is only granted when required by an individual's tasks, or when specifically authorized by an Act of Parliament or a Statutory Instrument</p> <p>f) The data processor must implement procedures/solutions for incident registration that enable the data controller to control the incident registers. All authorized use, any attempt at unauthorized use, as well as other breaches of security must be registered in the incident register.</p> <p><i>(see the example agreement and checklist below)</i></p>
4	<p>Data processing agreement follow-up</p> <p>The data controller must have access to the data processor's procedures for and operation of information security in order to ensure that these are satisfactory in terms of the requirements. It may in reality be difficult for a small health organization to gain such access. This is often because of a difference in size (an unequal power relationship) and/or differing levels of competence between the health organization and the external business unit.</p> <p>It is recommended that a practical solution to this problem is found when the agreement is being drawn up. For example, several smaller organizations may join together in gaining access to the relevant data processor documentation. Or one may agree that relevant results from the management review, security audits, and/or the handling of nonconformities are sent automatically to the data controller.</p> <p>It is important that the data controller, when entering into an agreement, makes certain demands of the external business unit. The following elements should be evaluated and described, depending on the needs of the organization:</p> <ul style="list-style-type: none"> - The data processor is duty bound to comply with the Code - The data processor is required to comply with standards such as the EPR standard, messaging standards, etc. - The data processor is required to comply with the organization's acceptance criteria (in accordance with the risk assessment) - The data processor is required to perform incident registration - The data processor is required to possess/comply with certain security certifications (e.g. ISO 27002) - Clear expressions of responsibility in relation to, amongst other things, the data being processed and how they are secured - The possibility of making changes to the data processing agreement (if the data controller's security audits of the data processor show that this is necessary)
5	<p>Duty of reporting</p> <p>The data processor must give regular status reports concerning the results within its areas of responsibility. This is particularly important if a data processor is being used. Elements that may be included in reports from the data processor (not exhaustive):</p>

No	Activity/Description
	<ul style="list-style-type: none"> - Number of logins to the system in question (authorized use) - Number of attempts to make unauthorized use of the system - Error situations - Uptime statistics - Nonconformities that may be found in the incident registers - Configuration changes
6	<p>Terminating a data processing agreement</p> <p>When the data processing agreement is terminated it is important that the data processor immediately returns all documents and electronic data in a readable format on the agreed medium (e.g. tape, CD, paper, etc.).</p> <p>When outsourcing the outsourcing agreement must include an agreement that health and personal data is to be returned to the data controller when the agreement is terminated.</p> <p>It is important to ensure that the data processor does not have any right to keep a copy of the data. It is recommended that the data controller receive a written confirmation stating that all health and personal data have been returned to the organization and that the data processor has not retained any copy, duplicate, or other reproduction of the data on any form of media.</p> <p>Finally, the data controller must ensure that the data processor remains bound by the duty of secrecy regarding the health and personal data processed even after the agreement has been terminated.</p> <p>Subsequent to the return of the health and personal data to the data controller, the data processor must delete the data from his system. The requirement to delete data includes any backups of the health and personal data.</p> <p>The Norwegian Data Protection Authority has stated that the systematic destruction of backups is not necessary if the data are erased through the rotation of backup media.</p> <p>The data processor must erase or securely destroy all documents, data, hard disks, CDs, and other storage media containing data covered by the agreement. The destruction must be carried out in such a manner that recovery of the data is impossible. This also applies to any backups and printouts that may exist.</p>

Example of a data processing agreement

The following is an example of text that should be included in an agreement between a tenderer and a supplier. As previously described, the text may form part of a contract, or be annexed to it. It is recommended that the example agreement is adapted to the circumstances of the agreement in question.

Data processing agreement between <organization> and <external business unit>

Purpose	Agreement ensuring that the requirements concerning confidentiality, integrity, and availability are met in accordance with the Patient Records Act and the Personal Data Act, including any regulations issued in pursuance of the latter act.
Conditions	That a thoroughly prepared agreement and other procedures are in place.
Date	<MM.DD.YYYY>
Version	<1.0>
Valid	<MM.DD.YYYY> to <MM.DD.YYYY>

<THE DATA PROCESSOR> is obliged to process personal data received from <THE DATA CONTROLLER> in such a manner that the requirements concerning confidentiality, integrity, and availability are met in accordance with the Patient Records Act sections 22 and 23, the Personal Data Act section 13, the Personal Data Regulations section 2-15, and the Code of conduct for information security.

It is the responsibility of <THE DATA CONTROLLER> to ensure that <THE DATA PROCESSOR>'s information security is satisfactory. If the level of security is unsatisfactory, <THE DATA PROCESSOR> must adjust the level of security as instructed by <THE DATA CONTROLLER>.

<THE DATA PROCESSOR> has the practical responsibility for ensuring that satisfactory information security has been established through planned and systematic measures. In relation to this <THE DATA PROCESSOR> must supply <THE DATA CONTROLLER> with documentation concerning its information security objectives and strategy.

When making use of suppliers for maintaining and updating filing systems, databases, etc., <THE DATA PROCESSOR> must ensure that these suppliers comply with the same requirements concerning information security. This must be done in such a manner that the level of information security, as described above, is not weakened. If health and personal data are to be transmitted through external networks these must be encrypted in line with existing regulations.

<THE DATA PROCESSOR> is required to document the system and procedures relevant to this agreement. By documentation is meant procedures for authorization and use, various technical and organizational measures. This documentation must be available to <THE DATA CONTROLLER>, the Data Inspectorate, and the Norwegian Board of Health Supervision. Access to the documentation must be strictly controlled (only given to a restricted number of authorized persons), so that this does not weaken the level of information security.¹

When information security nonconformities occur <THE DATA PROCESSOR> must, as part of the handling of nonconformities, send nonconformity reports to <THE DATA CONTROLLER>, insofar as the nonconformities are relevant for information security. <THE DATA CONTROLLER> has the right to let a third party audit <THE DATA PROCESSOR>'s information security. The costs of such an audit are to be covered by <THE DATA CONTROLLER>.

When the agreement is terminated the data processor must return documents and all electronic data on whatever medium (tape, CD, paper, etc) that <THE DATA PROCESSOR> is in possession of in its capacity as data processor. <THE DATA PROCESSOR> does not have any right to retain a copy of the material. <THE DATA CONTROLLER> shall receive a written confirmation from <THE DATA PROCESSOR> that all material has been returned to <THE DATA CONTROLLER>, and that <THE DATA PROCESSOR> has not retained any copy, duplicate, or other reproduction of the material on any medium.

The duty of secrecy concerning health and personal data and other relevant related information must be maintained for the duration of the agreement. The duty of secrecy also covers information concerning security measures (technically, physically, administratively, and organizationally). <THE DATA PROCESSOR> continues to be bound by the same duty of secrecy concerning the health and personal data processed even after the agreement has been terminated.

<Data controller>
<organization>

<Data processor>
<External business unit>

¹ It is recommended that fact sheets concerning the relevant service are referred to in the agreement (e.g. home office). The fact sheets are available at www.normen.no.

Example of a checklist of requirements of the data processor and the making of a data processing agreement

No	Requirement	Requirement met			Comment
		Yes	No	Not applicable	
1.	The data processor is required to comply with the Code and meet its requirements.				
2.	The data processor is required to comply with message standards where applicable.				
3.	The data processor must supply the data controller with a description of security objectives, security strategy, and responsibility for information security.				
4.	The data processor is required to process all information in line with the data processing agreement.				
5.	Requirements concerning incident registration:				
	- The data processor must ensure that all access to and use of ICT systems are registered in the incident register.				
	- Incident registers must be collected and made available to the data controller for queries and reports. The data controller shall determine which reports may be retrieved.				
	- Incident registers must be kept until such time as it is presumed that there will no longer be any use for them, based on the nature of the health care provided.				
	- The following must, at minimum, be registered in incident registers: <ul style="list-style-type: none"> o the authorized user's unique identifier o the authorized user's role when accessing o organizational affiliation o the organizational affiliation of the authorized user o the kind of information to which access has been provided o the reason(s) behind the access o time and duration of the access 				
6.	The data processor may not make use of subcontractors in relation to the processing of health and personal data unless the data controller has agreed in writing.				
7.	The data processor must ensure that the information processed on behalf of the data controller is kept separate from information and services belonging to itself or other organizations.				
8.	The data processor is required, in connection with the agreement, to document its system for processing health and personal data. By documentation is meant, amongst other things, description of procedures for authorization, authentication, and use, as well as technical and organizational security measures. The documentation must be made available to the data controller, the Data Inspectorate, and the Norwegian Board of Health Supervision.				
9.	The data processor must at all times comply with the information security requirements of the data processing agreement and the data controller's security strategy. The results of security audits must be presented to the data controller as documentation of the data processor's information security, as well as that of any subcontractors.				
10.	The data processor must ensure that the following minimum requirements are met (these requirements are not exhaustive):				
	- Access to network and ICT system services and				

No	Requirement	Requirement met			Comment
		Yes	No	Not applicable	
	information shall be on the basis of individual user names and passwords				
	- Information supplied by the data controller must be secured, ensuring that only authorized employees have access				
	- Access to external networks/Internet/health net, including the data processor's open network, must be secured through security measures that cannot be affected or sidestepped by external persons or the organization's employees, and which prevent the unwitting exposure of sensitive personal data to less secure networks				
	- When employing remote access all security measures and agreements must comply with the document 'Guidelines for remote access for maintenance and updates between supplier and health organization'				
	- Messages and data communications containing sensitive personal data must be encrypted				
	- If the data processor processes health and personal data on behalf of several organizations the data processor must ensure, through technical measures that cannot be overridden by the users, that the organizations are kept separate in accordance with the risk assessment. This applies to both databases in which data are stored and to communications				
11.	Access control requirements				
	- The data processor shall have procedures ensuring that only those employees of the data processor who have a genuine need for access to ICT systems and information for delivery/providing the service are authorized				
	- The data processor must at all times keep an account of employees authorized for access to the data controller's ICT systems and information. When requested such an account must be supplied to the data controller.				
	- If the data controller objects to a certain person having physical or electronic access to the ICT system, his authorization must be withdrawn				
	- Personal user accounts must be used for all access in connection with delivering the contract				
	- If the data processor utilizes portable equipment for operations, the data processor must implement procedures ensuring that such equipment is only used by operational personnel, and only for operational tasks				
	- If a third party or subcontractor is given access to the ICT system in connection with providing support services or the like, all security measures must be in compliance with the document 'Guidelines for remote access for maintenance and updates between supplier and health organization'				
12.	Duty of secrecy				
	- A duty of secrecy is imposed on the data processor's employees, and others operating on its behalf in connection with the processing of health and personal data in accordance with the data processing agreement, cf. the Patient Records Act section 15, the Health Personnel Act, and the Public Administration Act. The same applies to any subcontractors. The data processor must ensure that all persons processing health and personal data are cognizant of the duty of secrecy				

No	Requirement	Requirement met			Comment
		Yes	No	Not applicable	
	- All employees and others acting on behalf of the data processor in connection with the processing of health and personal data must have signed a duty of secrecy declaration. This also applies to any subcontractors				
	- The duty of secrecy continues to apply after the termination of the data processing agreement.				
	- The parties are required to take the necessary precautions in order to ensure that material or information is not disclosed to outside parties in violation of this article				
13.	<p>Reporting.</p> <p>The data processor shall provide regular reports concerning its areas of responsibility. Examples of what should be included in such reports:</p> <ul style="list-style-type: none"> - Operational status of critical systems - System uptime - Scheduled interruptions and their duration - Planned changes, expected effect, and time of execution - Attempts at unauthorized use - Security updates - Failures and corrections - Lack of compliance with the service agreement and possible causes 				