**Code of conduct for information security**
**www.normen.no**

Published with the support of:

Helsedirektoratet

# Use of test data in systems containing health and personal data

**Supporting document**
**Fact sheet no 43**
Version: 2.0
Date: 06 June 2013

| | | | |
|---|---|---|---|
| **Purpose** | The purpose of the fact sheet is to the ensure confidentiality, integrity, and availability when test data are used during the development and testing of IT systems containing health and personal data. | | |
| **Responsibility** | The manager of the organization is responsible for the safe handling of test data. The practical day-to-day responsibility may be delegated to e.g. the ICT manager. | | |
| **Execution** | When using test data in systems containing health and personal data during their creation, use, and deletion. | | |
| **Scope** | When test data will be created in connection with preparations, extraction, and use in order to comply with the requirements concerning personal data protection and information security. | | |
| **Target group**<br>This fact sheet is particularly relevant for: | ☐ Organization manager/management<br>☐ Person or body responsible for research<br>☐ Project manager – research<br>☒ Head of security/Security coordinator | ☐ Staff/employee<br>☐ Researcher<br>☒ Privacy protection ombudsman | ☒ ICT manager<br>☒ Data processor<br>☒ Supplier |
| **Authority** | The Personal Health Data Filing System Act section 16. | | |
| **References** | Code of conduct for information security. | | |

Testing systems, databases, and integrations are a central part of the development of new systems, upgrades, or troubleshooting. It is thus important to make use of relevant test data, in order that the tests may be as close to reality as possible.

If the organization is testing in accordance with a framework, the incorporation of the requirements and recommendations of this fact sheet in the framework documents is recommended.

Examples of the uses of test data

- Developing new systems
- Changing existing systems
- Verifying that new system versions do not corrupt data
- Testing new and existing integrations
- Identify the causes of operational problems such as bottlenecks that may arise subsequent to deployment, which again may cause reduced or lack of access to health and personal data
- Change of system of supplier that entails data conversion

A testing environment may be established as a permanent solution (copy of the production environment) or may only exist for a limited duration of time. Anonymized test data should be used where possible.

Basic requirements for the creation and use of test data

a) Persons primarily occupied with system development and maintenance shall normally not have access to health and personal data, but it is in the nature of things that they may nevertheless gain access through their work. Nevertheless the aim should be that such access should be as limited as possible. E.g. through the use of anonymized test data

b) The data controller shall ensure that external parties that may gain access to health and personal data comply with the requirements of the Code. Most external parties will be data processors, suppliers, or other health organizations.

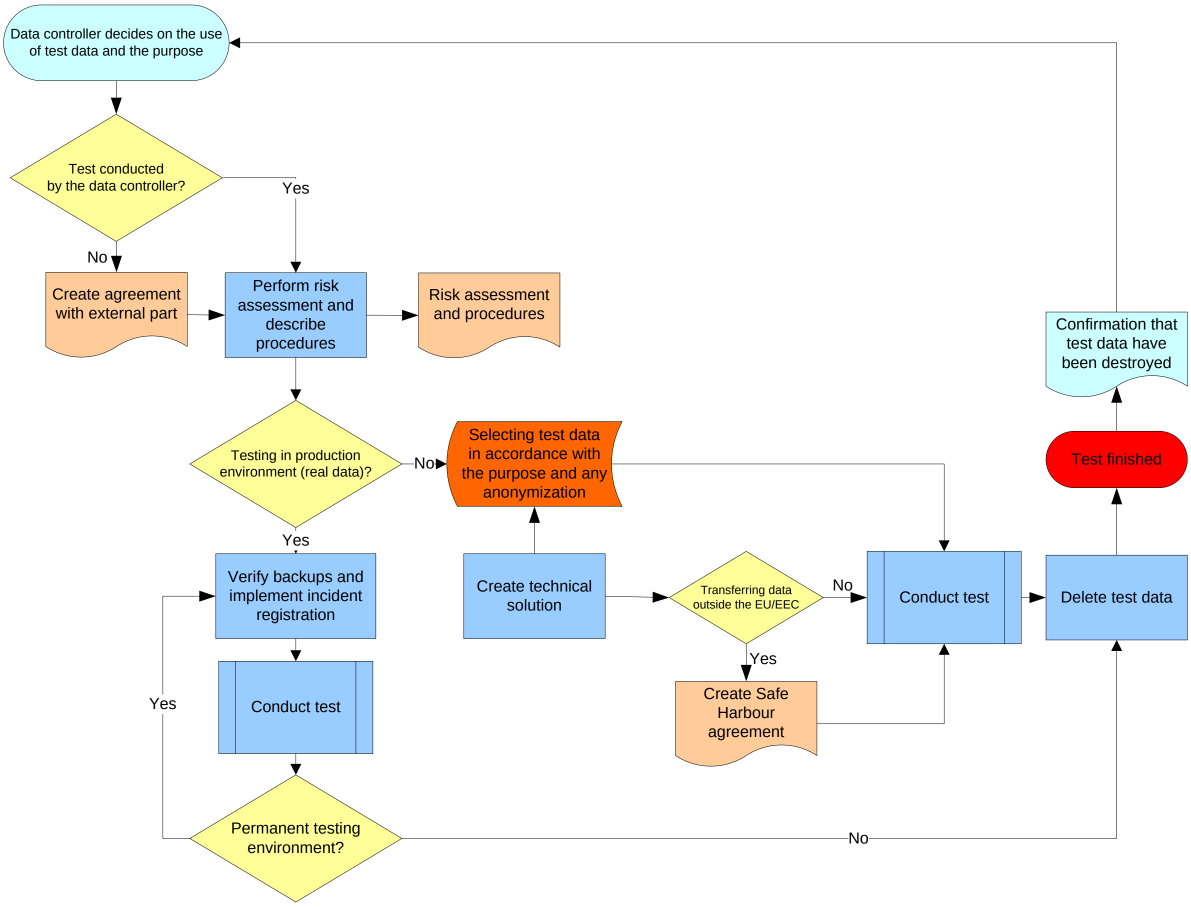
c) A written (data processing) agreement between the data controller and the party that may gain access to health and personal data must exist.

<u>Creation and use of test data</u>

| No | Action |
|---|---|
| 1. | **Preparations**<br>a) When using an external party to conduct testing the data controller must draw up a written agreement with the external party (data processor, supplier, organization) that will have access to the test data. The agreement must cover:<br>- The purpose and duration of the test (see above for examples)<br>- The Code applies and should be complied with<br>- The responsibilities of different roles (e.g. project manager's role)<br>- The use of identifiable health and personal data or anonymized data<br>- The selection of the whole or parts of the data set<br>- Separate testing environment or testing conducted on data in the production environment<br>- Who will have access to the test data and procedures for access control<br>- Duty of secrecy<br>- Performing risk assessment on the use of test data<br>- Physical and logical security<br>- Durability of test data and measures to ensure deletion of data when testing has concluded<br>- Which special procedures must be followed<br>b) Clarify roles:<br>- The responsibilities and tasks of various roles, both internally in the health organization and in the external party, must be clarified<br>c) Evaluate the use of identifiable or anonymized data:<br>- As a starting point, anonymized data should be used<br>- Use of identifiable data may take place for:<br>o Test conversion to maintain the integrity, where the main rule is that both the conversion and the test of the result must be conducted on real data in order to test a complete conversion<br>o Integrations where in most the causes the use of practically complete and real data is necessary in order to conduct a realistic communications test with external parties<br>d) Performing risk assessment of the testing environment:<br>- On the basis of the acceptance criteria the risk assessment should take into account the scope of health and personal data in the test data, the number of people having access to the test data, and the duration of the test<br>- The use of a separate testing environment or testing conducted on real data in the production environment<br>- Testing conducted on identifiable or anonymized data<br>- The physical testing environment<br>o Physical and logical separation of testing and production data<br>o Physical and logical production environment<br>- Access control, incident registration, and access control follow-up<br>e) When creating test data procedures shall be developed for:<br>- The selection of data from existing registers (e.g. EPR system)<br>- The anonymization of test data<br>- The use of test data<br>- Access control for test data<br>- Transferring test data to other parties (data processor, supplier, organization)<br>- The destruction of test data after testing is concluded |

| No | Action |
|---|---|
|  | f) Creating a technical solution for the processing of test data:<br>- A physical or logical (logically separated database) separation between the testing and production environment should be established unless the testing is conducted in the production environment<br>- The transfer of test data to a testing environment outside the data controller’s own network entails a greater exposure to risk. In order to do this in a secure manner mechanisms that ensure that data reach the correct recipient, and are made unavailable to outsiders through encryption should be implemented. As regards the strength of encryption, the Data Inspectorate’s current recommendation is recommended. When transferring a large amount of information, or in the case of repeated collaboration PKI based on qualified certificates should be used. Such systems will both ensure the correct authentication of the other party, safe transmission, and non-repudiation, to the extent that that is of importance. If identifiable test data are used a technical solution must be implemented and secured in the same manner as the production environment<br>- For testing of EDI messages, refer to KITH’s test server for messages: http://www.kith.no/templates/kith_WebPage____576.aspx |
| 2. | **Execution**<br>a) Selection of test data for the concrete purpose:<br>- Selection rules shall be described in accordance with the determined purpose<br>- The process of selecting test data must be secured in accordance with the Code. This is in reality a separate processing of health and personal data<br>- Test data shall be anonymized to greatest degree possible<br>b) Testing conducted on real data:<br>- Prior to testing the existence of backups and procedures for restoring data in the case the test corrupts data must be verified<br>- Incidents must be registered<br>- Manual incident registration of changes is recommended in order to be able to trace unwanted incidents to specific operations and times |
| 3. | **Closing/clean-up**<br>a) For time-limited use test data must be destroyed when the purpose has been achieved<br>b) In permanent testing environment test data no longer serving any purpose must be destroyed<br>c) The person responsible for the use of test data must send a confirmation to the data controller that all test data have been deleted in accordance with the purpose and agreement |

## Process flow illustration


Data controller decides on the use of test data and the purpose
Test conducted by the data controller?
Yes
No
Create agreement with external part
Perform risk assessment and describe procedures
Risk assessment and procedures
Testing in production environment (real data)?
No
Selecting test data in accordance with the purpose and any anonymization
Yes
Verify backups and implement incident registration
Create technical solution
Transferring data outside the EU/EEC
No
Conduct test
Delete test data
Yes
Create Safe Harbour agreement
Test finished
Confirmation that test data have been destroyed
Yes
Conduct test
Permanent testing environment?
No