Policies for distribution and management of data about test persons for SYSVAK

1 Introduction

In order to make implementation and test of the new SYSVAK system more efficient, Folkehelseinstituttet (FHI) intends to make available a small collection of test persons to manufacturers of systems which shall function as clients to SYSVAK.

The purpose of this document is to describe the conditions and policies under which this data shall be released from FHI, and instructions as to how it shall be managed by these manufacturers within their implementation and testing processes.

2 Generation of test collection

The collection of test persons has been generated by:

- beginning with several thousand data records from Folkeregister
- randomizing name and address data for these records; i.e., creating new associations between real names and real address
- extracting a small subset of these randomized records (ca. 100-200)
- generating "new" fødselsnummer for each record in the extract, such that these fødselsnummer are correctly constructed with respect to the algorithm for generation and assignment of fødselsnummer[1].
- for several of these test persons, artificial family relationships have been created; i.e., within a single person record, there may be data elements which refer to that person's mother and/or father: eventual references of this kind these parents are also members of the test collection.

3 Policies for distribution and management

3.1 Consent

FHI can deliver this collection of test persons to various manufacturers upon request. **By making such a request, the requesting organization implicitly consents to adhere to the policies and practices described below.**

3.2 Data delivery

This collection of test persons will be delivered as an encrypted zip file. The password for decryption shall be delivered via SMS. Therefore, the request for data must include the name of the contact person, as well as their email address and mobile number.

3.3 Data storage, access and destruction

The decrypted contents from the zip file must be stored on a server which is secured against unauthorized access. Any artifacts derived from that file (e.g., database tables, etc.) must also must be stored on a server which is secured against unauthorized access. Storage on any other temporary or permanent media storage device is prohibited.

[1] Ref. informasjon from Skatteetaten: "Generelt om folkeregistrering" (http://www.skatteetaten.no/Templates/Artikkel.aspx?id=6640&epslanguage=NO).

Access permission to the decrypted file, as well as any derived artifacts, must be limited to as few individuals as possible, and granted on an “only if needed” basis.

Upon successfully decryption and storage, the encrypted zip file must be immediately deleted/destroyed. When the implementation and testing processes is completed, the decrypted file and all derived artifacts must be deleted/destroyed.

3.4 Data backup

Any eventual backup copies of the decrypted file, as well as any derived artifacts, must be treated in the same manner as the original copies.

3.5 Distribution

Organizations receiving this collection of test persons from FHI may not re-distribute this data to any other actor under any circumstances. If such a need is encountered, organizations are requested to contact FHI in order that FHI can be responsible for data distribution.