

Copy No.

Doc Ref. **7163/T/1**  
Client **Icelandic Data Protection Authority**  
Project **Icelandic Health Database**  
Title **Security Target for an Icelandic Health Database**  
Date **31 January 2001**

**Review & Approval**

Issue: 1.4  
R&A Number: 7163/RA/8  
Originator:  
**John Arnold**  
Approval (PM):  
**Gary Smith**  
Approval (QAR):  
**Paul Morrison**

**Admiral Management Services Limited**  
Kings Court  
91-93 High Street  
Camberley  
Surrey GU15 3RN  
Tel: (01276) 686678  
Fax: (01276) 691028

© Copyright Admiral Management Services 2001

# Contents

## **1 Introduction**

- 1.1 General
- 1.2 Terminology
- 1.3 References

## **2 ST Introduction**

- 2.1 Identification
- 2.2 Overview and Scope
- 2.3 CC Conformance

## **3 TOE Description**

- 3.1 Overview of the TOE

## **4 Security Environment**

- 4.1 Assumptions
- 4.2 Threats
- 4.3 Organisational Security Policies

## **5 Security Objectives**

- 5.1 Security Objectives for the TOE
- 5.2 Security Objectives for the Environment

## **6 TOE Security Functional Requirements**

- 6.1 Introduction
- 6.2 Security Audit
- 6.3 Cryptographic Support
- 6.4 User Data Protection
- 6.5 Statistical Database Security
- 6.6 Identification and Authentication
- 6.7 Management of Functions in TSF
- 6.8 Protection of the TOE Security Functions
- 6.9 TOE Access

## **7 TOE Security Assurance Requirements**

- 7.1 Introduction
- 7.2 Assurance Requirements for the TOE
- 7.3 Assurance Requirements for the Environment
- 7.4 Strength of Function Requirement

## **8 TOE Summary Specification**

- 8.1 TOE Security Features
- 8.2 Assurance Measures

## **9 Rationale**

- 9.1 Security Objectives Rationale
- 9.2 Security Requirements Rationale
- 9.3 TOE Assurance Level Rationale
- 9.4 Environmental Assurance Level Rationale
- 9.5 Strength of Function Rationale

# 1 Introduction

## 1.1 General

1.1.1 This document proposes a Security Target (ST) for use with the Common Criteria (CC, ISO 15408).

1.1.2 A ST is a description of the security requirements for a particular IT system (or IT product). It describes the environment and purpose of the system, the threats against it and the security objectives of the system. It describes the system's security functional requirements (i.e. what the system must do). A ST must also describe the system's assurance requirements (i.e. how the system is to be developed and tested, so that those who rely upon the system can have confidence that it can be operated securely).

1.1.3 A ST follows the standard format for Security Targets defined in [CC].

1.1.4 A system can be evaluated against its ST, to show that:

- a) the system behaves as claimed in the ST functional requirements
- b) the system was developed and tested such that users can have the stated degree of assurance that no security flaws remain undiscovered.

1.1.5 To summarise, a ST can act as:

- a) a means of stating security requirements and claims
- b) a baseline for system development
- c) a baseline for system evaluation.

## 1.2 Terminology

1.2.1 This document uses the terminology of [CC]. Part 1 of the CC introduces some of the concepts underlying the CC and includes a glossary in section 2.3.

1.2.2 In this document, the present tense is used throughout.

1.2.3 The following terms are used in this ST with the stated meaning (see also Paragraphs 1.2.4 and 4.2.1.1):

- a) 'administrator' means an administrator of some aspect of the TOE, but excluding any aspect of the IES part of the TOE (which is administered by an 'IES administrator')
- b) 'environment' or 'operating environment' means the non-IT environment; and 'the DMU part of the TOE' (for example) means 'that part of the TOE that runs in the DMU environment, where the DMU environment means that part of the operating environment that is controlled by the DMU'
- c) 'indirect access' means access to IGG data via the QL, or access to IR data via the RDL
- d) 'microdata' means data derived from a database - considered as a table of rows (i.e. individuals) and columns (i.e. attributes, such as age) - within the TOE, where the derived data may include a copy of the value of an attribute (i.e. the type of data stored in a column) for one or more rows of the database
- e) 'macrodata' means statistical data calculated from microdata (e.g. the mean age of a group of people)

- f) 'query class' means a software module that translates a user request (for access to IGG/IR data), couched in the restricted query language defined by the query class, into the full query language used by the relevant database system; sends the translated request to the database system; and applies the required statistical inference countermeasures to the request, and to the response before it is returned to the user
- g) 'query' means a translated user request (see 'query class' definition above), e.g. an SQL sentence
- h) 'research proposal' means an application to the IEC for permission to access (indirectly) IGG data or to access (indirectly) IR data; a research proposal includes the query class(es) and the desired SIC control parameter values (see Section 6.5) to be used.

1.2.4 The following abbreviations are used in this ST:

CC	Common Criteria.
CM	Configuration Management.
DGPH	Director General of Public Health.
DMU	Database Maintenance Unit. In this ST, the term 'DMU' is used mainly to identify the physical environment that houses the hardware and software that run the IHD and the GLe and the GTe. The term may also refer to the organisation (currently the OLH) responsible for managing the IHD and the GLe and the GTe. (The union of the data stored in these three database systems is referred to as IGG data. The methodology used in joining data stored in these three database systems is subject to approval by the DPA.)
DPA	Data Protection Authority. An independent Icelandic agency, formerly known as the Data Protection Commission.
GL	Genealogy Database. An external (to the DMU) database dealing with genealogical information.
Gle	A database system which stores and processes data that is derived from source data in the external GL database.
GT	Genotype Database. An external (to the DMU) database dealing with individuals' genetic makeup.
Gte	A database system which stores and processes data that is derived from source data in the external GT database.
H	Health Database. A (logical) external (to the DMU) database dealing with individuals' health records.
IE	Íslensk erfðagreining ehf, an Icelandic company that has been granted a licence to create and operate the Icelandic Health Database and related hardware and software.
IEC	Interdisciplinary Ethics Committee. A body appointed by the Minister of Health and Social Security (see [Reg], Articles 25-29, also [Act], Article 12, Paragraph 3) to, <i>inter alia</i> , approve research proposals to query IGG data and IR data (via the QL and the RDL).
IES	Identity Encryption Service. This is a body controlled by the DPA. It is responsible for encrypting personal identification data during input (to the IHD and the GLe and the GTe) of information derived from the external H, GL and GT databases.
IHD	Icelandic Health Database. A central database system which stores and processes data that is derived from source data in the external H database. (IHD is considered to be synonymous with the term <i>Health Sector Database</i> , as implied by [Act], Article 10, Paragraph 2.)

IGG data	The union of the data stored in the three database systems IHD, GLe and GTe.
IR	Intermediate Results. A database containing results (of queries) returned by the QL.
IT	Information Technology.
MCHSD	Monitoring Committee on the Health Sector Database. May also be referred to as the Database Monitoring Committee. A body appointed by the Minister of Health and Social Security (see [Act], Article 6) to ensure that the creation and operation of the IHD are in keeping with the terms of [Act] and associated regulations and conditions, in so far as this does not fall within the ambit of the DPA.
OLH	Operating License Holder (currently IE).
PID	Personal Identification. Any data field that is intended to be used for the purpose of individual identification. According to [OpLic], Annex B (Transfer of Data to the HSD), Paragraph I.A.a, PID refers only to social security number.
PN	Personal Number. PN is a field in IGG data records. Two records containing the same PN data refer to the same person. The PN data is one-way encrypted so that it cannot be used for the purpose of individual identification as, for instance, an unencrypted PID could be.
QL	Query Layer. Software intended to process end-user requests for queries that are directed at IGG data.
RDL	Results Delivery Layer. Software intended to process customer requests for queries that are directed at IR data. (Note that the RDL returns macrodata only.)
SF	Security Function.
SFR	Security Functional Requirement.
SFP	Security Function Policy.
SIC	Statistical Inference Countermeasure.
SOF	Strength of Function.
ST	Security Target.
TL	Transfer Layer. Software intended to transfer (encrypted) data to the IES.
TOE	Target of Evaluation.
TSC	TSF Scope of Control.
TSF	TOE Security Functions. That part of the TOE which enforces security.
TSP	TOE Security Policy.

## 1.3 References

- [Act] Act on a Health Sector Database, Icelandic Parliament, Act No. 139/1998
- [BS7799] BS7799:1999 Information Security Management, BSI, 1999.
- [CC] ISO/IEC 15408-1:1999(E) Information Technology - Security Techniques – Evaluation Criteria for IT Security, Date: 1998 12-18
- [CEM] Common Methodology for IT Security Evaluation, CEM-991045, Part 2, Version 1.0, August 1999
- [DDXD.001] Technology, Security and Architecture: Concept and Requirements, IE, DDXD.001 Version 1.0, 31 August 1999
- [DDXD.002] Production and Operation of a Centralised Health Sector Database, IE, DDXD.002 Version 1.0, 31 August 1999
- [Denning] Cryptography and Data Security, Dorothy Denning, Addison Wesley, 1982
- [Keys] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, October 27 1999
- [OpLic] Operating Licence issued to Íslensk erfðagreining ehf for the Creation and Operation of a Health Sector Database, January 2000
- [Reg] Government Regulation on a Health Sector Database, Icelandic Government
- [Rowe] Diophantine Inference on a Statistical Database, Neil C. Rowe, Information Processing Letters, 18 (1984) 25-31
- [Terms] Technology, Security and Organisation Terms of the Icelandic Data Protection Commission in Relation to a Health-Sector Database, cf. Act No. 139/1998, Version No. 2, DPA, 19 January 2000 (also included in [OpLic] as Annex G).

## **2 ST Introduction**

### **2.1 Identification**

2.1.1 The title of this ST is **Security Target for an Icelandic Health Database**.

### **2.2 Overview and Scope**

2.2.1 This ST describes the security requirements of a database system (the IHD), and related hardware and software (such as the GLe and the GTe), being developed by the OLH. The Target of Evaluation (TOE) holds medical research data for the population of Iceland. The security requirements are primarily concerned with protecting the medical research data from unauthorised disclosure, but are also concerned with, for example, the process of transferring data from the health institutions and self-employed health workers to the IHD.

2.2.2 This ST is not concerned with ensuring the correctness, completeness or availability of the information stored in the TOE.

2.2.3 This ST includes rules for the management of the IHD. Data derived from the external GL and GT databases are covered because of a special provision in [Act] that they can be joined with the IHD. The methodology used in joining these databases is subject to approval by the DPA.

2.2.4 Note that, notwithstanding this document's title, the TOE encompasses more hardware and software than that used to store and process data derived from the external H database (see Paragraph 3.1.10).

2.2.5 Initial technical information about the TOE is given in [DDXD.001]. Higher level management and planning information is given in [DDXD.002]. These are English translations of IE's proposals as written in IE's application for the operating license, as required by [Act].

### **2.3 CC Conformance**

2.3.1 This section comments on the level of conformance between this ST and the CC.

2.3.2 The ST is part 2 extended, that is, it includes functional requirements which are not derived from Part 2 of the CC.

2.3.3 The ST is part 3 extended, that is, it is based on a recognised evaluation assurance level described in Part 3 of the CC, extended by non-standard assurance components. The ST also includes non-standard assurance components for evaluating the non-IT environment.

2.3.4 See Section 5.4 of the CC for more information about CC conformance statements.

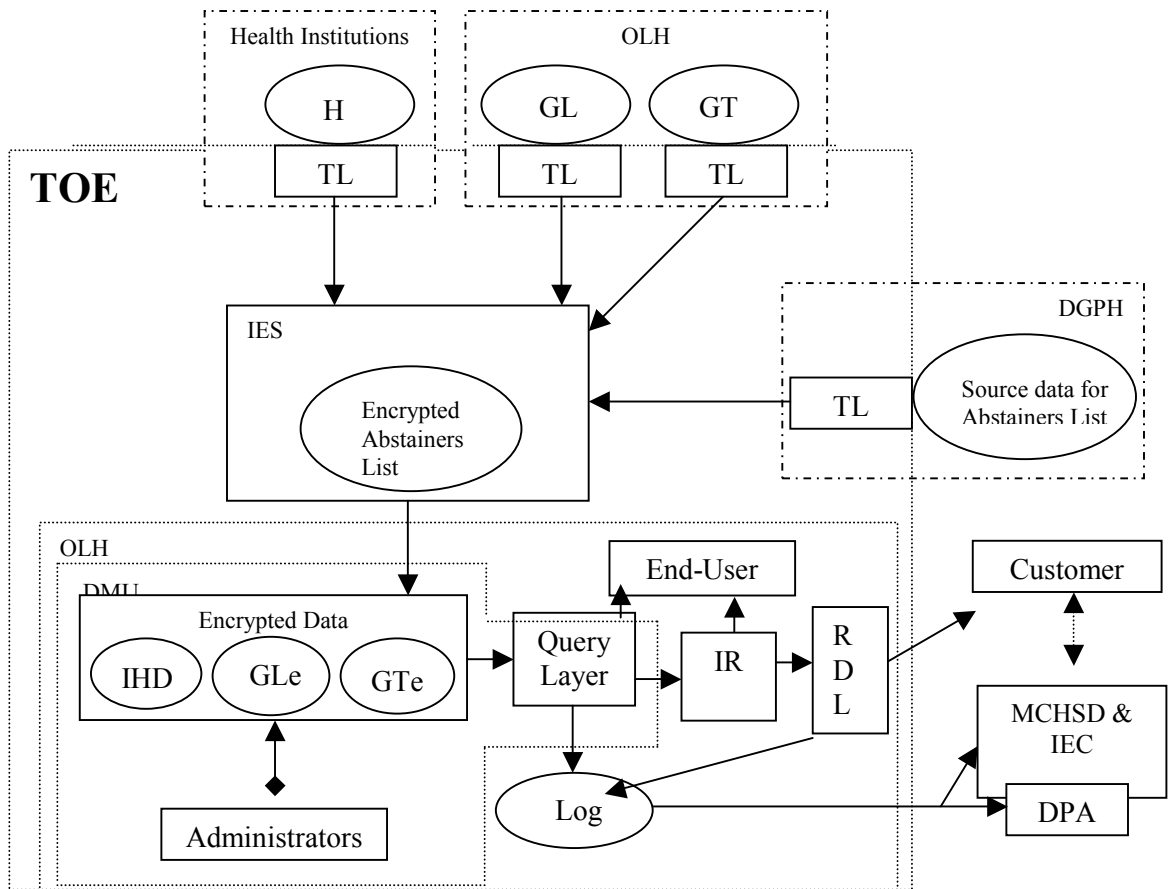
## 3 TOE Description

### 3.1 Overview of the TOE

- 3.1.1 The TOE is the IHD, a database system for storing and processing health data for research purposes, plus related hardware and software (such as the GLe and the GTe; see Paragraph 3.1.10 for further information). This ST also covers the special processes for joining data derived from the H, GL and GT databases, although the methodology used for joining requires a separate approval from the DPA. Data derived from the H database is held on the Icelandic population, except data generated (i.e. derived from the H database) for individuals after they have chosen to abstain from participation in the IHD (see [Act], Article 8).
- 3.1.2 The IHD is derived from records stored by health institutions and self-employed health workers.
- 3.1.3 The IHD can be joined to data derived from externally held databases containing genetic (GT) and genealogical (GL) information. The methodology for joining is subject to approval by the DPA (see [Act], Article 10, Paragraph 2).
- 3.1.4 Individuals can choose not to have data recorded about them in the IHD. An ‘abstainers list’ is maintained by the Director General of Public Health, which records the identities of people who have so chosen. No information derived from the H database is ever transmitted from the IES to the DMU (see Figure 3.1 overleaf) relating to any individual whose identity appears in the abstainers list. (Note that if an individual’s identity is added to the abstainers list after data relating to that individual has been recorded in the IHD, then no assertion is made as to whether or not that data continues to be recorded in the IHD.)
- 3.1.5 Data from all sources is anonymised by the IES before being input to the IHD or the GLe or the GTe. The IES also effects the abstainers list. The IES is managed by the DPA.
- 3.1.6 The DMU is the environment that houses the IHD and the GLe and the GTe (see also Paragraph 1.2.4). IGG data may be queried (indirectly) by end-users, in accordance with research proposals approved by the Interdisciplinary Ethics Committee (IEC). End-users cannot access the IHD or the GLe or the GTe directly. An end-user accesses IGG data indirectly via requests to the Query Layer (QL), and receives data known as Intermediate Results (IR) in response. An end-user may process his IR data (but not other end-users’ IR data) to investigate, for example, the correlation between certain attributes of groups of people. Such processing of IR data should be in accordance with the relevant research proposal, but it is not monitored to the same extent as the processing that is performed by the QL. However, an end-user submits requests to the QL using equipment that is located on OLH premises; this equipment does not provide the end-user with any facilities to remove (a copy of) any IR data from these OLH premises.
- 3.1.7 Customers are named staff of organisations such as pharmaceutical companies, research institutions, the Ministry of Health and Social Security, and the Director General of Public Health (DGPH). They cannot access the IHD or the GLe or the GTe or IR data directly, nor can they access the QL. A customer accesses IR data indirectly, in conjunction with an end-user (who may be the same individual person), as follows:
- a) the customer submits a research proposal to the IEC (in a similar fashion to the end-user)

- b) the end-user produces IR data, as outlined above, in the form that the customer wishes
- c) the customer then submits his own queries to this IR data, indirectly via requests to the Results Delivery Layer (RDL), and receives data in response. The RDL is similar to the QL, in that it is closely monitored, and it ensures that the requests and queries are permitted in accordance with the research proposal that relates to the IR data in question.

- 3.1.8 The MCHSD (see Paragraph 1.2.4) is appointed by the Minister of Health and Social Security. Its role is to monitor the creation and operation of the IHD and the GLe and the GTe, insofar as this does not fall within the ambit of the DPA, with assistance from the IEC (see Paragraph 1.2.4) and other independent experts as required. The MCHSD (in conjunction with the DPA) is responsible for ensuring compliance with the legislation and regulations relating to IGG data. The IEC controls the query classes that can be installed in the TOE.
- 3.1.9 Figure 3.1 shows, at a high level, the organisations/environments and (some of) the users involved in the input and output of data (see also Paragraph 4.1.4). The health institutions', DGPH and the GL/GT (if these reside outside the OLH) environments are outside the scope of this ST, but the functionality of the Transfer Layer (TL) - i.e. the software used to transfer (encrypted) data to the IES - is within the scope of the ST. (Note that the TL has to run within a suitable IT environment.)
- 3.1.10 The arrows on Figure 3.1 show the predominant data flow direction. The IT TOE is the implied hardware and software enclosed by the box labelled 'TOE'. The environment for the IT TOE (see Section 7.3) consists of the IES, the DMU and the OLH environments only. Administrators' interactions with parts of the TOE outside the DMU are omitted from Figure 3.1. 'Log' is audit records.
- 3.1.11 Note also that it is not necessarily a requirement that all the IHD and GTe and GLe data fields, once received into the DMU, be encrypted at all times. (However, PN data fields are encrypted at all times.)



**Figure 3.1: TOE and Relevant Organisations/Environments**

## 4 Security Environment

### 4.1 Assumptions

- 4.1.1 The IHD and the GLe and the GTe are intended to be used as statistical databases. Both in isolation and in combination, they should not divulge information about any identifiable person, only about groups of people with common biological properties.
- 4.1.2 The IHD and the GLe and the GTe are intended to be used for research into many areas of medical science, such as:
- a) basic research into genetics and disease
  - b) research into the relationship between genetics, diagnostics and treatment
  - c) analysis of the cost of disease and treatment
  - d) epidemiological studies.
- 4.1.3 The database(s) also develop Icelandic expertise in medical informatics, privacy protection of medical information and medical database design, which may be used in the future for consultancy in other projects.
- 4.1.4 The TOE runs in the following administrative domains (or environments):
- a) health institutions. These have the external H data, which is formatted, encrypted by the Transfer Layer, and passed to the IES. The health institutions must provide a suitable environment for the Transfer Layer to run, but that is outside the scope of this ST. The health institutions have been handling sensitive health data on computer for some time already, and are approved by the DPA to do so
  - b) the OLH (outside the DMU, see below). The OLH environment is subject to physical and procedural security measures. For convenience, it is assumed to include the external GL and GT data, which is encrypted by the Transfer Layer and passed to the IES. The OLH's handling of external GT and GL data is outside the scope of this ST. Its support for the Transfer Layer is within the scope of this ST. External GL and/or GT data could reside in another environment that is considered by the DPA to be suitably secure; for the purposes of this document, any such an environment is to be treated in the same manner as health institutions' environments
  - c) the DGPH. This generates the abstainers list. The data is encrypted by the Transfer Layer and passed to the IES. The DGPH's handling of raw data is outside the scope of this ST. Its support for the Transfer Layer is within the scope of this ST
  - d) the DMU. This is within the OLH environment, and is a more highly (than the rest of the OLH) secure environment in which the IHD and the GLe and the GTe run. The DMU provides the hardware and software to support the IHD and the GLe and the Gte and the QL. The DMU boundary may be extended to encompass other parts of the TOE
  - e) the IES. This is a highly secure environment in which PID encryption takes place. Its management and staff are independent of the OLH and the DMU.
- 4.1.5 The health institutions, OLH and DGPH environments are assumed to have adequate IT, personnel, physical and procedural controls in place to support the secure running of the Transfer Layer (TL).

4.1.6 In particular, it is assumed (ASS\_SEPARATE) that information providers are not able, as a result of the information preparation process, to relate personal identification data (e.g. name, address) to other data for any records for which they were unable to ascertain this relation prior to the information preparation process.

## 4.2 Threats

### 4.2.1 Agents

4.2.1.1 The threat agents, who may be in a position to attack the TOE, are of several different types (or classes). The classes are listed below, at two levels of granularity - e.g first level: item a), second level: item a)i). People in classes a)-h) inclusive are also referred to as (legitimate, or authorised) users:

- a) information provider staff. These are responsible for the source data from which the IHD and the GLe and the GTe and the abstainers list are derived. The following classes of information provider are envisaged:
  - i) staff at health institutions who prepare H data for transfer to the IHD
  - ii) staff at the OLH (or elsewhere, see Paragraph 4.1.4b) who maintain the GT and GL databases, and who prepare GT and GL data for transfer to the GTe and the GLe
  - iii) staff of the Director General of Public Health who maintain the abstainers list
- b) administrators. These are the people responsible for the day-to-day running and use of the TOE in general (apart from the IES), and of the IHD and the GLe and the GTe in particular. Currently, all administrators are OLH staff; any change from this situation requires the approval of the DPA. The following classes of administrator are envisaged:
  - i) access administrators (responsible for management of users, access controls and audit logs)
  - ii) operating system administrators
  - iii) database administrators
  - iv) hardware administrators
- c) end-users. These are people who query the IHD (and the GLe and the GTe, subject to the requirements of [Act], in particular, Article 10) indirectly via requests to the Query Layer in order to perform medical research. Each end-user has been vetted by the MCHSD and authorised by the MCHSD to submit queries to the IHD and GLe and GTe (indirectly via requests to the QL) in accordance with a research proposal that has been approved by the IEC. Members of the IEC may also choose to participate, with the MCHSD, in the above vetting and authorisation process
- d) customers. These are named staff of organisations, each of whom has been vetted by the MCHSD and authorised by the MCHSD to submit queries to IR data (indirectly via requests to the RDL) in accordance with a research proposal that has been approved by the IEC. Members of the IEC may also choose to participate, with the MCHSD, in the above vetting and authorisation process. The IR data in question is produced by an end-user
- e) IES staff. These run the IES. The following classes of IES staff are envisaged:
  - i) those who perform the normal functions of the IES (IES normal users)
  - ii) those responsible for management of the system (IES administrators)

- f) members of the DPA or MCHSD or IEC. These are (collectively) responsible for the following:
  - i) monitoring the operation of the IHD and the GLe and the GTe, and of the TOE in general
  - ii) approving research proposals, and hence approving the queries that each end-user can put to IGG data (indirectly via requests to the QL), and the queries that each customer can put to IR data (indirectly via requests to the RDL)
  - iii) monitoring compliance with this document
- g) pre-processor users. These are health professionals who are responsible for pre-processing H data that has been received at the DMU from the IES for inclusion in the IHD. They ‘clean’ the data with the aid of automated tools that, for instance, remove duplicate data
- h) key custodians. These are responsible for the update or input of the cryptographic keys used in the TOE. A key custodian may be responsible for all or part of a key, may be responsible for one or more keys, and may be a DPA employee
- i) persons without legitimate access to the TOE, such as Internet hackers. These may wish to damage the IHD or the GLe or the GTe, or access sensitive data on these database(s).

4.2.1.2 These (threat agent) classes (at the second level of granularity) must be kept separate, with the exception of DPA members and key custodians, and of end-users and customers. For instance, it must not be possible for a MCHSD member to be an end-user, nor can an access administrator be a database administrator. Each legitimate user is assigned to exactly one role (see Subsection 6.7.6), apart from information provider staff users (who are not assigned to any role), and:

- a) users who are both a DPA member and a key custodian (who are, therefore, assigned to both the DPA member and key custodian roles)
- b) users who are both end-users and customers (who are, therefore, assigned to both the end-user and customer roles).

## 4.2.2 Assets

4.2.2.1 The TOE must preserve the following assets:

- a) A\_DHD: any IGG data (including IR data derived from IGG data) within the TOE which can be related to the identity of the person the data applies to
- b) A\_IESDATA: operational data used inside the IES to restrict the set of individuals about whom data is transmitted from the IES to the DMU.

4.2.2.2 The ST is concerned with the confidentiality of A\_DHD. The integrity and availability of this data is outside the scope of this ST.

4.2.2.3 By its nature, IGG data (especially data derived from the H database) remains sensitive for a long time after its creation. When selecting generation algorithms and key lengths for cryptographic keys used in the TOE (particularly when the keys are used for the long-term storage of data), the OLH must consider not just the crypto-analytic technology that is currently available, but what may be developed in the foreseeable future.

4.2.2.4 The TOE must make proper use of the A\_IESDATA provided by the Director General of Public Health.

### 4.2.3 Attacks

4.2.3.1 As well as the well-understood attacks of impersonation and gaining access to data without authorisation, this TOE may be subject to some attacks that are unique to statistical databases.

4.2.3.2 These are referred to generically as 'statistical inference', which means processing statistical data, using techniques such as those described in Chapter 6 of [Denning], to violate privacy.

4.2.3.3 The computer security literature describes the following attacks, among others. This is not a complete list, and some of the attacks may not be applicable to the TOE, because of its static nature, and because of administrative controls:

- a) the tracker attack (Section 6.3.2 of [Denning]). This involves padding queries so that they pass the query set size restriction, then subtracting out the effect of the padding
- b) the linear system attack (Section 6.3.3 of [Denning]). This is a generalisation of the tracker attack and involves taking linear combinations of query results to reveal individual records
- c) the median attack (Section 6.3.4 of [Denning]). The median statistic always returns information about a single record. The attack relies upon finding two query sets with one common record and the same median
- d) insertion and deletion attacks (Section 6.3.5 of [Denning]). These involve inserting and deleting records to bypass query set size restrictions. These attacks are an issue when attackers can insert or delete individual records at will, which is not the case for this TOE
- e) diophantine attacks [Rowe]. This attack can be used when query sizes are small and the queryable statistics are based on some value which takes one of a small set of known values (such as integers). By solving a set of simultaneous diophantine equations it is sometimes possible to disclose individual record values, given a single statistic
- f) averaging. This is an attack against data perturbation. It attempts to remove noise by averaging over many queries.

4.2.3.4 Note that the analysis of potential attacks on a statistical database given in [Denning] assumes that repeated and unconstrained queries are permitted to be submitted to the (publicly accessible) database, which leads to the derivation of the counter-measures given in the reference. However, for this TOE, such assumptions are largely negated by the technical and procedural access controls defined and anticipated by this security target; and this fact allows some flexibility in specifying and applying the appropriate SICs.

#### **4.2.4 Threats**

- 4.2.4.1 The following are the threats against which the TOE must protect itself.
- 4.2.4.2 T\_IMPERSONATE: an attacker may attempt to impersonate a legitimate TOE user and gain his privileges within the TOE without authorisation.
- 4.2.4.3 Anyone may attempt to perform this attack. Hackers may perform it out of curiosity; legitimate users may wish to gain additional privileges or to avoid being held accountable for their actions.
- 4.2.4.4 The effect of a successful attack would be a loss of accountability with TOE users.
- 4.2.4.5 T\_DIRECT: an attacker may attempt to directly link data to the person it applies to and thereby effect an unauthorised disclosure.
- 4.2.4.6 Anyone may attempt this attack. To perform this attack successfully, it is necessary to have access to unencrypted personal data. If the TOE and its environment function correctly, it limits attackers to the following categories:
- a) end-users, who access IGG data via the QL
  - b) customers, who access IR data via the RDL
  - c) information provider staff, who have access to the records they are preparing. This is outside the scope of this ST because these staff already have access to this data, and it is assumed (ASS\_SEPARATE) that they are not able, as a result of the information preparation process, to relate personal identification data (e.g. name, address) to other data for any records for which they were unable to ascertain this relation prior to the information preparation process
  - d) pre-processor users, who have access to unencrypted data for pre-processing
  - e) anyone who can impersonate the above.
- 4.2.4.7 The effect of a successful attack would be that embarrassing or damaging information about individuals would be made public, and confidence in the TOE would be lost.
- 4.2.4.8 T\_STATISTIC: an attacker may attempt to statistically infer sensitive data about an identified individual.
- 4.2.4.9 To perform this attack in practice, it is necessary to have (indirect) access to the database(s) or IR data. This is only available to:
- a) end-users
  - b) customers
  - c) anyone who can impersonate the above.
- 4.2.4.10 Note that information provider staff do not have the capability to submit (directly or indirectly) queries to the IHD or the GLe or the GTe or IR data.
- 4.2.4.11 The effect of a successful attack would be the same as for T\_DIRECT.
- 4.2.4.12 T\_FILTER: MCHSD and DPA and IEC staff may negligently or deliberately fail to properly define and control access to query classes. Clearly, this threat only applies to MCHSD and DPA and IEC staff.
- 4.2.4.13 The effect of a successful attack would be that it may become easier to perform T\_STATISTIC attacks.

- 4.2.4.14 T\_COMMS: an attacker may attempt to compromise the TOE's security by monitoring or tampering with communications over insecure lines.
- 4.2.4.15 This threat applies to anyone with access to the communications media used by the TOE. This applies particularly to telcos and their employees, but could potentially include anyone with Internet access.
- 4.2.4.16 The effect of a successful attack would be that sensitive data could be accessed before being input to the TOE, with a similar result to T\_DIRECT.
- 4.2.4.17 T\_AUDIT: following an attack, it may be impossible to detect the attack, or to trace it to its source. This threat is not related to a particular threat agent.
- 4.2.4.18 The effect of an audit failure would be to lessen the accountability provided by the TOE, and to reduce the deterrent against attacking the TOE.
- 4.2.4.19 T\_ABSTAIN: the TOE may permit the transfer of data, from the IES to the DMU, about a person against his wishes. This threat is not related to a particular threat agent.
- 4.2.4.20 The result of this event would be to lessen confidence in the TOE.

### **4.3 Organisational Security Policies**

- 4.3.1 There are no organisational security policies.

## **5 Security Objectives**

### **5.1 Security Objectives for the TOE**

5.1.1 The TOE has one principal security objective:

- a) OBT\_PROT to protect personally identifiable data from disclosure.

5.1.2 The TOE also has some subsidiary security objectives:

- a) OBT\_AUTH to verify the claimed identities of TOE users
- b) OBT\_ABSTAIN to allow persons to choose not to have data (derived from the H database) about them transmitted from the IES to the DMU
- c) OBT\_COMMS to protect sensitive data in transit
- d) OBT\_AUDIT to keep records of TOE events and activities so that security abuses can be detected and traced to their origins.

### **5.2 Security Objectives for the Environment**

5.2.1 The security objectives of the DMU and OLH and IES environments are:

- a) OBE\_ACCOUNT to provide a binding between IT entities (e.g. usernames, key certificates) and the real world entities (natural or corporate persons) corresponding to them
- b) OBE\_ROLE to separate the roles of the TOE (with the exception of DPA member and key custodian, and of end-user and customer), so that, for instance, no one can simultaneously be (or have the privileges of) a MCHSD member and an end-user
- c) OBE\_PHYSICAL to provide physically secure DMU and OLH and IES environments
- d) OBE\_PROCEDURE to provide users with rules and guidance on the secure use of the TOE so that they do not inadvertently compromise the TOE's security
- e) OBE\_QUERY to ensure that permitted query classes of the TOE:
  - i) are useful
  - ii) conform to ethical criteria
  - iii) do not allow statistical inference
- f) OBE\_TRUST to ensure by personnel measures that TOE users can be trusted not to abuse their capabilities within the TOE
- g) OBE\_SUPERVISE to ensure that hardware administrators are supervised by at least one other type of administrator whenever they are given access to hardware containing sensitive data.

5.2.2 These requirements form the baseline for the environmental assessment defined in Section 7.3.

# 6 TOE Security Functional Requirements

## 6.1 Introduction

6.1.1 This chapter specifies the functional requirement components of this ST. Most of these components are taken from the CC Part 2 (e.g. FAU\_ARP.1 Security Alarms), in which case their elements are quoted in full, subject to the following conventions:

- a) the results of permitted operations (on the text) are given in square brackets []
- b) in some cases the wording has been slightly changed (without changing the meaning) in order to preserve correct English syntax.

6.1.2 Requirement components that extend those from the CC Part 2 have identifiers beginning with "ST\_". For example, ST\_QUERY\_SIZE (see Section 6.5).

6.1.3 In addition (to security functional requirements), note the following restrictions on the TOE's implementation:

- a) the IHD and the GLe and the GTe database systems shall execute on dedicated computer(s); in particular, the QL software shall execute on a different computer from those computer(s) that host the IHD and GLe and GTe
- b) an end-user shall submit requests to the QL using a workstation that is located on OLH premises. The workstation shall provide no facilities to the end-user (in respect of IR data accessible to the end-user from this workstation) for printing data, or for copying data to or from any magnetic media that is intended to be removeable (e.g. a floppy disk), or for copying data between any computers other than the workstation and the computer(s) that host the IR data.

## 6.2 Security Audit

### 6.2.1 FAU\_ARP.1 Security Alarms

6.2.1.1 The TSF shall [inform an access administrator] upon detection of a potential security violation within the DMU or the OLH parts of the TOE.

6.2.1.2 Note that the CC term 'potential security violation' equates to 'potential violation of the TSP', see Subsection 6.2.4.

### 6.2.2 FAU\_GEN.1 Audit Data Generation

6.2.2.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) start-up and shut-down of the audit functions
- b) all auditable events for the [detailed] level of audit.

6.2.2.2 The TSF shall record within each audit record at least the following information:

- a) data and time of the event, event type, subject identity, and the outcome (success or failure) of the event
- b) for each audit event type, based on the auditable event definitions of the functional components included in the ST, [the information given below.

6.2.2.3 For this TOE, the detailed level of audit includes the following:

- a) actions taken due to imminent security violations [FAU\_ARP.1]
- b) enabling and disabling of any of the audit analysis mechanisms, and any automated responses performed by the tool [FAU\_SAA]
- c) failed or successful attempts to read audit records, with search parameters used [FAU\_SAR]

- d) modifications to the audit configuration that occur while the audit collection functions are operating [FAU\_SEL.1]
- e) actions taken due to audit storage failure [FAU\_STG.4]
- f) success and failure of cryptographic operations (excluding any sensitive cryptographic material) [FCS]
- g) all attempts to perform an operation on an object covered by the access control SFP, with the specific security attributes used to perform the access check [FDP\_ACF.1]
- h) all attempts to transfer data between physically separated parts of the TOE, including any integrity errors that occurred and actions taken upon detection of an integrity error [FDP\_ITT]
- i) all requests (from end-users and customers) received by the QL or the RDL; in each case the required information includes the complete request, the end-user's or customer's identity, the query class used, whether the request was accepted or rejected, and:
  - i) for accepted requests, the SIC control parameters used and the response returned [SICs in Section 6.5]
  - ii) (deleted)
- j) changes to the default or minimum/maximum allowed values for the SICs' control parameters specified in Section 6.5
- k) (deleted)
- l) reading, addition, update and deletion of database records by the pre-processor users
- m) (deleted)
- n) creation, deletion and modification of query classes [query class SFP]
- o) changes to access permissions for a query class, including the original and final permissions [query class SFP]
- p) blacklisting and resetting of blacklist status [FIA\_AFL.1]
- q) acceptance or rejection by the TSF of any tested secrets (no sensitive data to be audited) [FIA\_SOS]
- r) any changes to the defined quality metrics [FIA\_SOS]
- s) all use of authentication mechanisms, with detailed reasons for any failures [FIA\_UAU]
- t) all use of the user identification mechanism, including the user identity provided [FIA\_UID]
- u) success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject) [FIA\_USB]
- v) all modifications in the behaviour of the functions in the TSF [FMT\_MOF]
- w) all modifications to the values of security attributes [FMT\_MSA.1]
- x) modifications to the rules or parameters for setting initial values of security attributes [FMT\_MSA.3]
- y) all modifications to the values of TSF data, including rejections [FMT\_MTD]
- z) specification of expiration times [FMT\_SAE]

- aa) modification of the group of users that are part of a role [FMT\_SMR]
- bb) unsuccessful attempts to use a role due to the given conditions on the roles [FMT\_SMR]
- cc) use of the rights of a role [FMT\_SMR]
- dd) execution of tests of the underlying machine and results of those tests [FPT\_AMT]
- ee) (deleted)
- ff) (deleted)
- gg) changes to the time [FPT\_STM]
- hh) providing a timestamp [FPT\_STM]
- ii) execution of TSF self tests and results of the tests [FPT\_TST.1]
- jj) rejection of a new session based on the limitation of multiple concurrent sessions [FTA\_MCS]
- kk) capture of the number of concurrent user sessions and the user security attributes of each one [FTA\_MCS]
- ll) locking of an interactive session by the session locking mechanism [FTA\_SSL]
- mm) successful unlocking of an interactive session [FTA\_SSL]
- nn) any attempts at unlocking an interactive session [FTA\_SSL].

### **6.2.3 FAU\_GEN.2 User Identity Association**

6.2.3.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### **6.2.4 FAU\_SAA.1 Potential Violation Analysis**

6.2.4.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

6.2.4.2 The TSF shall enforce the following rules for monitoring audited events:

- a) accumulation or combination of [queries to the IHD or the GLe or the GTe or IR data, particularly repeated queries to a fixed subset], known to indicate a potential security violation
- b) [creation, deletion or modification of database records by the database administrator
- c) creation, modification, deletion, re-ordering or replay of data in transit between physically separate parts of the TOE
- d) repeated authentication failures].

### **6.2.5 FAU\_SAR.1 Security Audit Review**

6.2.5.1 The TSF shall provide [MCHSD and DPA and IEC members] with the capability to read [all information] from the audit records.

6.2.5.2 The TSF shall provide the audit records in a manner suitable for the [MCHSD and DPA and IEC members] to interpret the information.

### **6.2.6 ST\_AUDIT Audit Records Not Sensitive**

6.2.6.1 The TSF shall not record any information (e.g. microdata) in the audit records that could lead to disclosure of personally identifiable data.

### **6.2.7 FAU\_SAR.2 Restricted Audit Review**

6.2.7.1 The TSF shall prohibit all users' read access to the audit records, except those users that have been granted explicit read-access.

### **6.2.8 FAU\_SAR.3 Selectable Audit Review**

6.2.8.1 The TSF shall provide the ability to perform [searches] of audit data based on [any combination of the following]:

- a) the user who caused the event
- b) event type
- c) date and time interval, time of day, day of the week
- d) request (for IGG/IR data) and response text].

### **6.2.9 FAU\_SEL.1 Selective Audit**

6.2.9.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

- a) [event type].

### **6.2.10 FAU\_STG.1 Protected Audit Trail Storage**

6.2.10.1 The TSF shall protect the stored audit records from unauthorised deletion.

6.2.10.2 The TSF shall be able to prevent modifications of the audit records.

### **6.2.11 FAU\_STG.4 Prevention of Audit Data Loss**

6.2.11.1 The TSF shall [prevent auditable events, except those requested by an access administrator] if the audit trail is full.

## **6.3 Cryptographic Support**

### **6.3.1 FCS\_CKM.1 Cryptographic Key Generation**

6.3.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet the following:

- a) [when a random number generator is used in the key generation process, all values shall be generated randomly or pseudo-randomly such that all possible combinations of bits and all possible values are equally likely to be generated
- b) a seed key, if used, shall be input in the same way as cryptographic keys
- c) intermediate key generation states and values shall not be accessible outside of the cryptographic module in plain text or otherwise unprotected form].

### **6.3.2 FCS\_CKM.2 Cryptographic Key Distribution**

6.3.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method that meets the following:

- a) [a secure cryptographic key negotiation protocol shall be used].

### **6.3.3 FCS\_CKM.3 Cryptographic Key Access**

6.3.3.1 The TSF shall perform [input, output and storage of keys] in accordance with a specified cryptographic key access method that meets the following:

- a) [keys shall be stored either encrypted or in a hardware cryptographic module

- b) access to update or input the keys shall be restricted to the authorised key custodian(s)
- c) manually distributed secret and private keys shall not be input to or output from a cryptographic module in plain text form. Rather, they shall be input or output either:
  - i) encrypted; or
  - ii) via a smartcard; or
  - iii) using split knowledge procedures (i.e. as two or more plain text key components). In this case, the module shall have the capability to separately authenticate the two users involved. The key components shall be input directly into the module or output directly from it, without travelling through any enclosed or intervening systems where components could be stored, combined or otherwise processed
- d) electronically distributed secret and private keys shall be input and output in encrypted form].

### **6.3.4 FCS\_CKM.4 Cryptographic Key Destruction**

6.3.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method that meets the following:

- a) [all cryptographic modules used shall provide the capability to zeroise all plain text cryptographic keys and other sensitive material within the module].

### **6.3.5 FCS\_COP.1 Cryptographic Operation**

6.3.5.1 The TSF shall perform [encryption] in accordance with specified cryptographic algorithm(s) and cryptographic key size(s) that meet the following:

- a) [the strength of function requirement for the TOE].

6.3.5.2 Note that the use of encryption within the TOE must satisfy the relevant requirements of [Act] (see, for example, Article 7); in particular it is necessary that:

- a) health data is transferred to the IES, and from the IES to the DMU, in encrypted form (and remains encrypted within the IES)
- b) personal identification (which is, in general, data used to form a PN) is encrypted one-way (starting with its transfer to the IES, and being further encrypted in the IES).

## **6.4 User Data Protection**

### **6.4.1 The IGG/IR Data SFP**

6.4.1.1 This subsection outlines the SFP (or access control policy) to be adopted for user data (in this case, the union of data in, or being transferred to, the IHD and the GLe and the GTe, plus the abstainers list, plus IR data) handled by the TOE. First, the different classes of user and data are identified. Then, the access allowed between these is defined.

6.4.1.2 The user classes distinguished for this policy are those (legitimate) user classes of Paragraph 4.2.1.1.

6.4.1.3 The classes of (unencrypted) data distinguished for this policy are as follows:

- a) D\_IR: Intermediate Results (IR) data:
- b) D\_PM: health data (less any personal identification data)
- c) D\_CR: genealogical and genetic data (less any personal identification data)

d) D\_AB: the abstainers list.

6.4.1.4 The above classes refer to unencrypted data only, excluding the source data from which they are derived. Encrypted IGG data plus encrypted abstainers list data is treated in this ST as system data and is covered under the FPT\_SEP security functional requirements. Note that personal identification data is always encrypted.

6.4.1.5 The following are the types of access that can be provided to data:

- a) RW: read-write access
- b) L: limited read-write access via tools for data cleaning. To be classified as 'limited access' the pre-processor tools must enforce the following:
  - i) pre-processor users shall not be able to choose which records to access
  - ii) pre-processor users shall be shown only one record at a time
  - iii) pre-processor users shall only be shown information that they need for the purposes of their immediate task
  - iv) pre-processor users shall not be given access to any information in the accessed records which could be used for identification (e.g. address)
  - v) each tool shall have an obvious data-cleaning purpose
  - vi) tool use and record access are audited
- c) Q: access via installed query classes, as defined in the Query Class SFP (see next subsection).

6.4.1.6 The following table defines the access allowed between users (subjects) and data (objects), with the following restrictions:

- a) one end-user cannot access IR data that is derived from a user request submitted by another end-user
- b) during an end-user's given *login session*, the IR data that the end-user is permitted to access is IR data that relates to one research session only, where:
  - i) 'login session' means 'the period between the end-user successfully logging in to, and logging out from, the TOE'
  - ii) 'IR data that relates to' means 'IR data that is derived from user request(s) submitted as part of'
- c) a customer's access to IR data is limited to IR data that is derived from a request submitted for IGG data by an end-user on behalf of that customer.

<b>Table 6.1 IGG/IR Data SFP (see also Paragraph 6.4.1.6)</b>				
User Class	D_IR	D_PM	D_CR	D_AB
Information providers at OLH				
Information providers at health institutions				
Information providers at the DGPH				
Key custodians				
Access administrators				
Operating system administrators				
Database administrators				
Hardware administrators				
IES normal users				
IES administrators				
Pre-processor users		L		
Customers	Q			
MCHSD/DPA/IEC members				
End-users	RW	Q	Q	

**6.4.2 The Query Class SFP**

6.4.2.1 A query class is as defined in Section 1.2. Note that a query class includes the allowed values of the SIC control parameters (see Section 6.5).

6.4.2.2 Queries to IGG or IR data can be submitted on behalf of end-users or customers only via a query class (that is installed in the QL or RDL). Each installed query class is associated with access permissions which determine who (if anyone) is allowed to request a query belonging to that class. Hence, query classes and their associated access permissions control the ability to access (indirectly) the IHD or the GLe or the GTe or IR data.

6.4.2.3 The user classes distinguished for this policy are those (legitimate) user classes of Paragraph 4.2.1.1.

6.4.2.4 The classes of data distinguished for this policy are as follows:

- a) D\_QC: query classes.

6.4.2.5 The following are the types of access that can be provided to data:

- a) CMD: creating, modifying and deleting query classes
- b) A: specifying access permissions between users and query classes
- c) Eql: executing a query class that is installed in the QL, subject to having permission to do so
- d) Erdl: executing a query class that is installed in the RDL, subject to having permission to do so.

6.4.2.6 The following table defines the access allowed between users (subjects) and data (objects). Note that the results of operations performed by users with CMD and A access to D\_QC have to be in accordance with decisions made by the DPA/MCHSD/IEC (see Paragraph 7.3.7.11).

<b>Table 6.2 Query Class SFP</b>		
User Class	D_QC	
Information providers at OLH	A	
Information providers at health institutions		
Information providers at the DGPH		
Key custodians		
Access administrators		
Operating system administrators		
Database administrators		CMD
Hardware administrators		
IES normal users		
IES administrators		Erdl
Pre-processor users		
Customers		
MCHSD/DPA/IEC members		
End-users	EqI	

**6.4.3 FDP\_ACC.2 Complete Access Control**

- 6.4.3.1 The TSF shall enforce the [IGG/IR data and query class SFPs] on [the subjects and objects identified in the SFPs] and all operations among subjects and objects covered by the SFPs.
- 6.4.3.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by the IGG data and query class SFPs.

**6.4.4 FDP\_ACF.1 Security Attribute Based Access Control**

- 6.4.4.1 The TSF shall enforce the [IGG/IR data and query class SFPs] to objects based on [the class of the user requesting the access and the class of the data being accessed].
- 6.4.4.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
  - a) [see Tables 6.1-2].
- 6.4.4.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:
  - a) [none].
- 6.4.4.4 The TSF shall explicitly deny access of subjects to objects based on the [following additional rules:
  - a) none].

**6.4.5 FDP\_ITT.1 Basic Internal Transfer Protection**

- 6.4.5.1 The TSF shall enforce the [IGG/IR data and query class SFPs] to prevent the [disclosure] of user data when it is transmitted between physically-separated parts of the TOE.

**6.4.6 FDP\_ITT.3 Integrity Monitoring**

- 6.4.6.1 The TSF shall monitor user data transmitted between physically-separated parts of the TOE for the following errors:
  - a) [modification
  - b) deletion

c) reordering

d) replay.]

6.4.6.2 Upon detection of a data integrity error, the TSF shall:

a) [terminate the connection].

**6.4.7 FDP.RIP.2 Full Residual Information Protection**

6.4.7.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.

**6.4.8 ST\_ABST Abstaining**

6.4.8.1 The TSF shall contain an ‘abstainers list’ specifying persons who have chosen to abstain from (further) participation in the IHD.

6.4.8.2 The TSF shall not transmit any data derived from the H database from the IES to the DMU relating to any personal identification that occurs in the abstainers list.

6.4.8.3 The TSF shall store the abstainers list in encrypted form so that it is impossible to determine who is on the list.

## 6.5 Statistical Database Security

### 6.5.1 Introduction

- 6.5.1.1 This section specifies the countermeasures to be taken to protect the data in the IHD and the GLe and the GTe, plus IR data, from statistical inference attacks. These countermeasures are regularly and frequently reviewed in collaboration with the DPA and MCHSD and IEC, to ensure protection of privacy and, as far as possible, the usability of the TOE.
- 6.5.1.2 For more information on the rationale for these countermeasures, see the literature on computational disclosure control and statistical inference control, e.g. the following sections in [Denning]:
- a) for ST\_PERT, see 6.5.3
  - b) for ST\_QUERY\_SIZE, see 6.3.1
  - c) for ST\_SUBSET, see 6.5.2.
- 6.5.1.3 The statistical inference countermeasures (SICs) that are specified in this section are intended to be implemented within the TOE's Query Layer and/or Results Delivery Layer (see Section 3.1). Each SIC has associated control parameter(s), and each control parameter can be set, for each query class, to specify a range of values. There are two stages to implementing and using a new query class:
- a) firstly, the DPA has to agree that the query class may be installed (i.e. that the QL software and/or the RDL software may be upgraded)
  - b) secondly, the IEC has to agree that the query class may be used, by vetting all research proposals (which state, *inter alia*, the query classes that are desired to be used).
- 6.5.1.4 The only way that an end-user can submit a query to IGG data is via a query class installed in the QL. The QL ensures that the query, and the results of the query (prior to being returned to the end-user), comply with the SICs' control parameter settings for the query class used. In the case of non-compliance the QL returns only a message to that effect to the end-user. The RDL functions in a similar manner with respect to a customer and IR data.
- 6.5.1.5 The SICs and their control parameters are intended to give the IEC the flexibility to allow, on a case by case basis, appropriate access to IGG data such that the results returned allow the end-user to conduct meaningful research, without compromising the privacy and anonymity of any individual's data; and similarly for a customer and IR data.
- 6.5.1.6 In general, each of a SIC's control parameter(s) may be set to a range of values. For some control parameters the upper and lower values of the range would normally be set to be identical; also, a control parameter may be set so that, in effect, the SIC is not applied (for the query class in question). For example, the ST\_SUBSET control parameter range could be set to be 100%-100%, or the ST\_PERT control parameter could be set to be null. However, it is intended (see Subsection 6.5.2) that the QL is configured such that some SICs are invariably applied for each query class, thereby preventing an end-user from making repeated and unconstrained queries to IGG data; and similarly for a customer and IR data.

6.5.1.7 The SICs are specified below. Note that, with respect to the ST\_SUBSET SIC, it is intended that any sampling applied to the IHD also applies indirectly to the GLe. In other words, a query directed to the GLe applies to a subset of the GLe that corresponds to the group of individuals represented by the result of a query previously directed to the IHD.

## **6.5.2 ST\_GEN General SIC Requirements**

6.5.2.1 The TOE shall include, as part of its Query Layer and Results Delivery Layer (see Section 3.1), a number of installed query classes (see Subsection 6.4.2). The TSF shall ensure that each installed query class includes, for each SIC control parameter, a range of control parameter values.

6.5.2.2 The TSF shall enforce the following restrictions on SIC control parameters, for each query class:

- a) the ST\_PN\_CHANGE control parameter (i.e. research session definition) must always be set; in other words, the ST\_PN\_CHANGE SIC must always be applied
- b) the ST\_QUERY\_SIZE control parameter must never be set to less than ten (see [Terms], Article 5, which states ‘No data shall be provided on fewer than ten patients at each time’)
- c) the ST\_STATS control parameter must never be set to allow microdata to be returned to a customer (via the RDL).

6.5.2.3 The TSF shall ensure that, for each query that is processed by the QL or the RDL, the following conditions are satisfied:

- a) the query, and the results of the query (prior to being returned to the end-user or customer), comply with the SICs’ control parameter settings for the query class used
- b) in the case of non-compliance, the TSF shall ensure that the only information returned as a result of the query is a message stating that no results are available; this message may also include a reason, e.g. ‘Insufficient records found’.

## **6.5.3 ST\_PERT Data Perturbation**

6.5.3.1 The TSF shall provide a means to randomly modify exact statistical values.

6.5.3.2 The form and size of the perturbation shall be a SIC control parameter for each query class.

## **6.5.4 ST\_QUERY\_SIZE Query Set Size Restriction**

6.5.4.1 For each query submitted, the TSF shall calculate the number of data records (i.e. records with differing PNs) that would be used in forming the response, along with the complement (i.e. the number of data records that would not be used in forming the response). If either of the following conditions is true, then the TSF shall treat the query as being non-compliant (see Paragraph 6.5.2.3 above):

- a) the number is greater than zero and less than the minimum query set size for the query class
- b) the complement is zero and this is not allowed, or the complement is greater than zero and less than the minimum query set size for the query class.

6.5.4.2 The minimum query set size, and whether a complement of zero is allowed, shall be a SIC control parameter for each query class. See also Paragraph 6.5.2.2b) above.

## **6.5.5 ST\_STATS Statistical Data Restriction**

6.5.5.1 For each query submitted, the TSF shall limit the response to macrodata unless the ST\_STATS control parameter indicates that microdata may (also) be included in the response.

6.5.5.2 Whether or not microdata may be included in the response to a query shall be a SIC control parameter for each query class. See also Paragraph 6.5.2.2c) above.

#### **6.5.6 ST\_SUBSET Operating on a Subset of the Database(s)**

6.5.6.1 The TSF shall provide a means to limit the result (of a query) to a sample of the complete IHD and a sample of the complete GTe. The sample(s) shall be chosen unpredictably, either randomly or pseudo-randomly.

6.5.6.2 The proportion of records to be included in the sample(s) shall be a SIC control parameter for each query class.

#### **6.5.7 ST\_PN\_CHANGE Prevent Tracking of PNs in Different Sessions**

6.5.7.1 The TSF shall ensure that the results of queries submitted in different *research sessions* (see next paragraph) cannot be related to each other via PN values.

6.5.7.2 The definition of a research session, in terms of its duration (e.g. submission of one query, or submission of several queries of the same class), shall be a SIC control parameter for each query class. See also Paragraph 6.5.2.2a) above.

#### **6.5.8 ST\_ATTR\_EXCL Attribute Exclusion**

6.5.8.1 For each query submitted, the TSF shall ensure that each attribute (of an data record) that is referenced in the query (either as part of the search criterion or as part of the data to be returned) is permitted to be included in the query. If the query references an attribute that is excluded (i.e. not permitted), then the TSF shall treat the query as being non-compliant (see Paragraph 6.5.2.3 above).

6.5.8.2 The attribute(s) to be excluded from a query shall be a SIC control parameter for each query class.

#### **6.5.9 ST\_ATTR\_GRAN Define Attribute Granularity**

6.5.9.1 For each query submitted, the TSF shall ensure that the result for each attribute that would be used in forming part of the response is given in terms of a granularity of the attribute that is within the range permitted for that attribute.

6.5.9.2 The permitted (range of) granularity (for each attribute that is relevant to the query class in question) shall be a SIC control parameter for each query class.

#### **6.5.10 ST\_MIN\_MULT Define Minimum Multiplicity of Attributes**

6.5.10.1 The following definitions are used in this subsection:

- a) a multiplicity for an attribute is a number of (a given subset of) data records that share the same value for that attribute
- b) the least multiplicity for an attribute is the smallest such number
- c) a multiplicity, and the least multiplicity, for a group of attributes are defined in the same way as for a single attribute
- d) the minimum multiplicity for an attribute or group of attributes is a number.

6.5.10.2 For each query submitted, the TSF shall do the following, in respect of each attribute or group of attributes that is a member of the relevant SIC control parameter list (see next paragraph):

- a) calculate the least multiplicity, considering the number of data records (i.e. records with differing PNs) that would be used in forming the response

- b) if this number is less than the minimum multiplicity for that attribute or group of attributes, then treat the query as being non-compliant (see Paragraph 6.5.2.3 above).

6.5.10.3 A list of attributes and/or groups of attributes, together with a minimum multiplicity for each member of the list, shall be a SIC control parameter for each query class. The default value of the control parameter shall be an empty list.

#### **6.5.11 ST\_NONDET Non-deterministic Choice of Records**

6.5.11.1 For each query submitted, the TSF shall, in respect of each attribute that is part of the search criterion, check that the attribute value used lies within a permitted range. If any of these checks fail, then the TSF shall treat the query as being non-compliant (see Paragraph 6.5.2.3 above).

6.5.11.2 The permitted range of values, in respect of each attribute that may be used as part of the search criterion, shall be a SIC control parameter for each query class.

### **6.6 Identification and Authentication**

#### **6.6.1 FIA\_AFL.1 Authentication Failure Handling**

6.6.1.1 The TSF shall detect when [3] consecutive unsuccessful authentication attempts occur related to [login].

6.6.1.2 When the defined number of consecutive unsuccessful authentication attempts has been met or surpassed, the TSF shall [blacklist the user so that no further logins by him are possible, until an authorised IES or access administrator has reset his blacklist status].

#### **6.6.2 FIA\_ATD.1 User Attribute Definition**

6.6.2.1 The TSF shall maintain the following set of security attributes belonging to individual users:

- a) [name
- b) contact details
- c) contract details for access to the IHD and the GLe and the GTe and IR data
- d) authentication information
- e) permitted login times and locations
- f) permitted inactivity duration
- g) time of last successful login
- h) number of unsuccessful login attempts since last successful login
- i) blacklist status].

#### **6.6.3 FIA\_SOS.1 Verification of Secrets**

6.6.3.1 The TSF shall provide a mechanism to verify that [passwords] meet [the following requirements:

- a) passwords must have a length of at least 16 characters
- b) passwords must contain at least one lower case alphabetic, at least one upper case alphabetic, and at least one numeric].

#### **6.6.4 ST\_FIRST\_PW Confidentiality of Secrets**

6.6.4.1 The TSF shall protect authentication secrets against discovery by all threat agents.

- 6.6.4.2 The TSF shall generate a user's initial password randomly.
- 6.6.4.3 The TSF shall not display the initial password to anyone, but shall print it on a tamper-evident envelope such that the password cannot be seen without visibly opening the envelope.

#### **6.6.5 FIA\_UAU.2 User Authentication before any Action**

- 6.6.5.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### **6.6.6 FIA\_UAU.4 Single-use Authentication Mechanisms**

- 6.6.6.1 The TSF shall prevent reuse of authentication data related to [the user's token].

#### **6.6.7 FIA\_UAU.5 Multiple Authentication Mechanisms**

- 6.6.7.1 The TSF shall provide [passwords, tokens or biometric devices, as appropriate] to support user authentication.

- 6.6.7.2 The TSF shall authenticate any user's claimed identity according to any two of:

- a) [his knowledge of his password
- b) his possession of his token
- c) a biometric aspect of the user allowing reliable authentication].

#### **6.6.8 FIA\_UAU.7 Protected Authentication Feedback**

- 6.6.8.1 The TSF shall provide only [echoing a fixed character while entering a password] to the user while the authentication is in progress.

#### **6.6.9 FIA\_UID.2 User Identification before any Action**

- 6.6.9.1 The TSF shall require each user to identify himself before allowing any TSF-mediated actions on behalf of that user.

#### **6.6.10 FIA\_USB.1 User Subject Binding**

- 6.6.10.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

### **6.7 Management of Functions in TSF**

#### **6.7.1 FMT\_MOF.1 Management of Security Functions Behaviour**

- 6.7.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [of the TSF as follows:

- a) maintenance of the rules for detecting a potential security violation - access administrator [FAU\_SAA]
- b) maintenance of the criteria for audit selection - IES or access administrator [FAU\_SEL]
- c) selecting the methods used to protect data during transmission - IES or access administrator [FDP\_ITT.1]
- d) resetting blacklisted users - IES or access administrator [FIA\_AFL]
- e) management of user tokens and authentication data - IES or access administrator [FIA\_SOS]
- f) management of user identities - IES or access administrator [FIA\_UID, FIA\_ATD]

- g) managing the expiration times for tokens and passwords - IES or access administrator [FMT\_SAE]
- h) managing the TSF self-test functions - IES, operating system and database administrators [FPT\_TST]
- i) hardware and network infrastructure management - IES or hardware administrator
- j) general operating system management, backup and restore - IES or operating system administrator
- k) general database management - database administrator
- l) management of query classes – database administrator
- m) management of cryptographic keys - key custodian [FCS\_CKM]].

## **6.7.2 FMT\_MSA.1 Management of Security Attributes**

6.7.2.1 The TSF shall restrict the ability to [modify] the security attributes as follows:

- a) [the classes ( or roles) to which users are assigned, and the access rules they must satisfy - IES or access administrator [FDP\_\*], [FMT\_SMR]
- b) the current time - IES, access or operating system administrator [FPT\_STM]
- c) the maximum allowed number of concurrent user sessions by a user - IES or access administrator [FTA\_MCS]
- d) the duration of user inactivity after which lock-out occurs (both for an individual user, and the default) - IES or access administrator [FTA\_SSL]
- e) the access banner - IES or access administrator [FTA\_TAB]].

## **6.7.3 FMT\_MSA.3 Static Attribute Initialisation**

6.7.3.1 The TSF shall provide [restrictive] default values for security attributes that are used to enforce the SFPs.

6.7.3.2 The TSF shall allow the [IES or access administrators] to specify alternative initial values to override the default values when an object or information is created.

## **6.7.4 FMT\_MTD.1 Management of TSF Data**

6.7.4.1 The TSF shall restrict the ability to [modify] the [configuration data of the TSF] to [authorised users as follows:

- a) authentication retry limit - IES or access administrator [FIA\_AFL]
- b) user attributes (name, contact details, contract details, permitted login times) - IES or access administrator [FIA\_ATD]
- c) the quality metric used for user secrets - IES or access administrator [FIA\_SOS]].

## **6.7.5 FMT\_SAE.1 Time-limited Authorisation**

6.7.5.1 The TSF shall restrict the capability to specify an expiration time for [passwords and tokens] to [the IES or access administrator].

6.7.5.2 For each of these security attributes, the TSF shall be able to [prevent the owner from logging in successfully] after the expiration time for the indicated security attribute has passed.

## **6.7.6 FMT\_SMR.2 Restrictions on Security Roles**

6.7.6.1 The TSF shall maintain the roles:

- a) [IES administrator
- b) IES normal user
- c) access administrator
- d) operating system administrator
- e) database administrator
- f) hardware administrator
- g) key custodian
- h) pre-processor user
- i) MCHSD/IEC member
- j) DPA member
- k) end-user
- l) customer].

6.7.6.2 The TSF shall be able to associate users with roles.

6.7.6.3 The TSF shall ensure that the following conditions are satisfied:

- a) [that the database administrator must be authorised to login each time by the access administrator
- b) that the database administrator cannot access the operating system or security configuration data
- c) that the operating system administrator cannot access the databases or security configuration data
- d) that the access administrator cannot access non-security-related database or operating system data
- e) that no administrator has any rights within the IES part of the TOE, and the IES administrator has no rights within the DMU or OLH parts of the TOE
- f) that no key custodian has access to any data encrypted by a key he holds].

## **6.8 Protection of the TOE Security Functions**

### **6.8.1 FPT\_AMT.1 Abstract Machine Testing**

6.8.1.1 The TSF shall run a suite of self tests [during initial start-up] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

### **6.8.2 (Deleted)**

6.8.2.1 (Deleted)

### **6.8.3 FPT\_RVM.1 Non-bypassability of the TSP**

6.8.3.1 The TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the TOE is allowed to proceed.

**6.8.4 FPT\_SEP.1 TSF Domain Separation**

6.8.4.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

6.8.4.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

**6.8.5 FPT\_STM.1 Reliable Time Stamps**

6.8.5.1 The TSF shall be able to provide reliable time stamps for its own use.

**6.8.6 FPT\_TST.1 TSF Testing**

6.8.6.1 The TSF shall exercise a suite of self tests at the request of an authorised administrator to demonstrate the correct operation of the TSF.

6.8.6.2 The TSF shall provide an authorised administrator with the capability to verify the integrity of TSF data.

6.8.6.3 The TSF shall provide an authorised administrator with the capability to verify the integrity of stored TSF executable code.

## **6.9 TOE Access**

### **6.9.1 FTA\_MCS.1 Basic Limitation on Multiple Concurrent Sessions**

6.9.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

6.9.1.2 The TSF shall enforce, by default, a limit of [1] sessions per user.

### **6.9.2 FTA\_SSL.1 TSF-initiated Session Locking**

6.9.2.1 The TSF shall lock an interactive session after [the user's permitted inactivity duration has expired] by:

- a) clearing or overwriting display devices, making the current contents unreadable
- b) disabling any activity of the user's data access/display devices other than unlocking the session.

6.9.2.2 The TSF shall require the following events to occur prior to unlocking the session: [re-authentication].

### **6.9.3 FTA\_SSL.2 User-initiated Locking**

6.9.3.1 The TSF shall allow user-initiated locking of the user's own interactive session, by:

- a) clearing or overwriting display devices, making the current contents unreadable
- b) disabling any activity of the user's data access/display devices other than unlocking the session.

6.9.3.2 The TSF shall require the following events to occur prior to unlocking the session: [re-authentication].

### **6.9.4 FTA\_TAB.1 Default TOE Access Banners**

6.9.4.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

### **6.9.5 FTA\_TAH.1 TOE Access History**

6.9.5.1 Upon successful session establishment, the TSF shall display the [date, time and location] of the last successful session establishment to the user.

6.9.5.2 Upon successful session establishment, the TSF shall display the [date, time and location] of the last unsuccessful attempt at session establishment and the number of unsuccessful attempts since the last successful session establishment.

6.9.5.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

# 7 TOE Security Assurance Requirements

## 7.1 Introduction

7.1.1 This chapter specifies the assurance requirements for the TOE and its environment by reference to [CC] Part 3, to which the reader should turn for more information.

## 7.2 Assurance Requirements for the TOE

### 7.2.1 Introduction

7.2.1.1 The base assurance requirements for this ST are EAL3 - methodically tested and checked. This level is extended by requiring the TOE to meet the requirements of AVA\_VLA.3 for statistical inference countermeasures. It is also augmented by upgrading from ACM\_SCP.1 to ACM\_SCP.2.

7.2.1.2 For each component, the developer action elements from Part 3 of [CC] are included. The Content and Presentation of Evidence elements, and the Evaluator Action elements, are given in Part 3 of [CC].

7.2.1.3 Where developer or evaluator actions call for sampling, a sampling rate of 5-10% shall be deemed sufficient.

### 7.2.2 ACM\_CAP.3 Authorisation controls

7.2.2.1 The developer shall provide a reference for the TOE.

7.2.2.2 The developer shall use a configuration management system.

7.2.2.3 The developer shall provide configuration management documentation.

### 7.2.3 ACM\_SCP.2 Problem tracking CM coverage

7.2.3.1 The developer shall provide configuration management documentation.

### 7.2.4 ADO\_DEL.1 Delivery Procedures

7.2.4.1 The developer shall document procedures for delivery of the TOE or parts of it to the user.

7.2.4.2 The developer shall use the delivery procedures.

### 7.2.5 ADO\_IGS.1 Installation, generation and start-up procedures

7.2.5.1 The developer shall document the procedures necessary for the secure installation, generation and start-up of the TOE.

### 7.2.6 ADV\_FSP.1 Informal functional specification

7.2.6.1 The developer shall provide a functional specification.

### 7.2.7 ADV\_HLD.2 Security enforcing high-level design

7.2.7.1 The developer shall provide the high-level design of the TSF.

### 7.2.8 ADV\_RCR.1 Informal correspondence demonstration

7.2.8.1 The developer shall provide an analysis of correspondence between adjacent pairs of TSF representations that are provided.

### 7.2.9 AGD\_ADM.1 Administrator guidance

7.2.9.1 The developer shall provide administrator guidance addressed to system administrative personnel.

- 7.2.10 AGD\_USR.1 User guidance**
  - 7.2.10.1 The developer shall provide user guidance.
- 7.2.11 ALC\_DVS.1 Identification of security measures**
  - 7.2.11.1 The developer shall produce development security documentation.
- 7.2.12 ATE\_COV.2 Analysis of coverage**
  - 7.2.12.1 The developer shall provide an analysis of test coverage.
- 7.2.13 ATE\_DPT.1 Testing: high level design**
  - 7.2.13.1 The developer shall provide an analysis of the depth of testing.
- 7.2.14 ATE\_FUN.1 Functional testing**
  - 7.2.14.1 The developer shall test the TSF and document the results.
  - 7.2.14.2 The developer shall provide test documentation.
- 7.2.15 ATE\_IND.2 Independent testing - sample**
  - 7.2.15.1 The developer shall provide [access to] the TOE for testing.
- 7.2.16 AVA\_MSU.1 Examination of Guidance**
  - 7.2.16.1 The developer shall provide guidance documentation.
- 7.2.17 AVA\_SOF.1 Strength of TOE security function evaluation**
  - 7.2.17.1 The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of function claim.
- 7.2.18 AVA\_VLA.1 Developer Vulnerability Analysis**
  - 7.2.18.1 The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.
  - 7.2.18.2 The developer shall document the disposition of obvious vulnerabilities.
- 7.2.19 AVA\_VLA.3 Moderately Resistant**
  - 7.2.19.1 The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the statistical inference countermeasures specified in Section 6.5.
  - 7.2.19.2 The developer shall document the disposition of identified vulnerabilities.
- 7.3 Assurance Requirements for the Environment**
  - 7.3.1 Introduction**
    - 7.3.1.1 The assurance level for the environment is based on EAL1 - functionally tested. The requirements are given in full below because their wording has been changed to make them suitable for non-IT assurance.
    - 7.3.1.2 The basic EAL1 requirements have been augmented by additional requirements for configuration management, ACM\_CAP.3 and ACM\_SCP.2.
    - 7.3.1.3 For each component, the full definition from Part 3 of [CC] is included, amended as necessary.
  - 7.3.2 ACM\_CAP.3 Authorisation controls**
    - 7.3.2.1 *Developer Action Elements*
    - 7.3.2.2 The developer shall provide a reference for the environment.

- 7.3.2.3 The developer shall use a configuration management system.
- 7.3.2.4 The developer shall provide configuration management documentation.

- 7.3.2.5 *Content and Presentation of Evidence Elements*
- 7.3.2.6 The reference for the environment shall be unique for each version of the environment.
- 7.3.2.7 The CM documentation shall include a configuration list and a CM plan.
- 7.3.2.8 The configuration list shall describe the configuration items that comprise the environment.
- 7.3.2.9 The CM documentation shall describe the method used to uniquely identify the configuration items.
- 7.3.2.10 The CM system shall uniquely identify all configuration items.
- 7.3.2.11 The CM plan shall describe how the CM system is used.
- 7.3.2.12 The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
- 7.3.2.13 The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
- 7.3.2.14 The CM system shall provide measures such that only authorised changes are made to the configuration items.
- 7.3.2.15 *Evaluator Action Elements*
- 7.3.2.16 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 7.3.3 ACM\_SCP.2 Problem tracking CM coverage**
- 7.3.3.1 *Developer Action Elements*
- 7.3.3.2 The developer shall provide CM documentation.
- 7.3.3.3 *Content and Presentation of Evidence Elements*
- 7.3.3.4 The CM documentation shall show that the CM system, as a minimum, tracks the following: policy documentation, test documentation, user documentation, administrator documentation, CM documentation and security flaws.
- 7.3.3.5 The CM documentation shall describe how configuration items are tracked by the CM system.
- 7.3.3.6 *Evaluator Action Elements*
- 7.3.3.7 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 7.3.4 ADO\_IGS.1 Installation, generation and start-up procedures**
- 7.3.4.1 This component has been omitted as it is irrelevant for an environment.
- 7.3.5 ADV\_FSP.1 Information security policy**
- 7.3.5.1 *Developer Action Elements*
- 7.3.5.2 The developer shall provide an informal security policy.
- 7.3.5.3 *Content and Presentation of Evidence Elements*
- 7.3.5.4 The policy shall describe the environment and its practices and procedures using an informal style.
- 7.3.5.5 The policy shall be internally consistent.

- 7.3.5.6 The policy shall describe the purpose and method of use of all environmental practices and procedures, providing details of effects and exceptions, as appropriate.
- 7.3.5.7 The policy shall completely represent the security relevant parts of the environment.
- 7.3.5.8 The policy's structure and content shall conform to [BS7799].
- 7.3.5.9 *Evaluator Action Elements*
- 7.3.5.10 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 7.3.5.11 The evaluator shall determine that the policy is an accurate and complete instantiation of the TOE's security objectives for the environment.
- 7.3.5.12 The evaluator shall determine that the policy provides adequate support for the secure operation of the TOE.
- 7.3.6 ADV\_RCR.1 Informal correspondence demonstration**
- 7.3.6.1 *Developer Action Elements*
- 7.3.6.2 The developer shall provide an analysis of correspondence between adjacent pairs of environmental documents that are provided.
- 7.3.6.3 *Content and Presentation of Evidence Elements*
- 7.3.6.4 For each adjacent pair of provided environmental documents, the analysis shall demonstrate that all relevant functionality of the more abstract representation is correctly and completely refined in the less abstract representation.
- 7.3.6.5 *Evaluator Action Elements*
- 7.3.6.6 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 7.3.7 AGD\_ADM.1 Administrator guidance**
- 7.3.7.1 *Developer Action Elements*
- 7.3.7.2 The developer shall provide administrator guidance addressed to administrative personnel.
- 7.3.7.3 *Content and Presentation of Evidence Elements*
- 7.3.7.4 The administrator guidance shall describe the administrative practices and procedures available to the administrator of the environment.
- 7.3.7.5 The administrator guidance shall describe (with warnings where necessary) how to administer the environment in a secure manner.
- 7.3.7.6 The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to the secure operation of the environment.
- 7.3.7.7 The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
- 7.3.7.8 The administrator guidance shall describe each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the environment.
- 7.3.7.9 The administrator guidance shall be consistent with all other documentation supplied for evaluation.
- 7.3.7.10 The administrator guidance shall describe all security requirements for the environment that are relevant to the administrator.

- 7.3.7.11 The administrator guidance shall include procedures for translating decisions made by the DPA/MCHSD/IEC into modifications of the TOE's behavior – in particular, modifications of the Query Layer's behaviour and the Results Delivery Layer's behaviour.
- 7.3.7.12 *Evaluator Action Elements*
- 7.3.7.13 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 7.3.8 AGD\_USR.1 User guidance**
- 7.3.8.1 *Developer Action Elements*
- 7.3.8.2 The developer shall provide user guidance.
- 7.3.8.3 *Content and Presentation of Evidence Elements*
- 7.3.8.4 The user guidance shall describe the practices and procedures available to the non-administrative users of the environment.
- 7.3.8.5 The user guidance shall describe (with warnings where necessary) the use of user practices and procedures available in the environment.
- 7.3.8.6 The user guidance shall clearly present all user responsibilities necessary for secure operation of the environment, including those assumptions regarding user behaviour that are stated in the ST.
- 7.3.8.7 The user guidance shall be consistent with all other documentation supplied for evaluation.
- 7.3.8.8 The user guidance shall describe all security requirements for the environment that are relevant to the user.
- 7.3.8.9 *Evaluator Action Elements*
- 7.3.8.10 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 7.3.9 ATE\_IND.1 Independent audit - conformance**
- 7.3.9.1 *Developer Action Elements*
- 7.3.9.2 The developer shall provide access to the environment for auditing.
- 7.3.9.3 *Content and Presentation of Evidence Elements*
- 7.3.9.4 The environment shall be suitable for auditing.
- 7.3.9.5 *Evaluator Action Elements*
- 7.3.9.6 The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 7.3.9.7 The evaluator shall audit a subset of the environment as appropriate to confirm that the environment is managed as specified.

## 7.4 Strength of Function Requirement

7.4.1 The TOE shall provide a minimum strength of function of **SOF-high**. This is taken to mean that the TOE shall resist attackers with the following capabilities:

- a) powerful software development capability
- b) knowledge of computer security and hacking techniques (including attacks against statistical databases, see [Denning])
- c) capacity to eavesdrop on and tamper with communications on long-distance telecommunications networks
- d) knowledge of the TOE's internal structures and protocols
- e) knowledge of public domain crypto-analytic techniques
- f) the attacker can be any legitimate TOE user, or if he is not a legitimate user, the attacker can collude with any legitimate TOE user. Collusion between two or more legitimate TOE users is excluded as a likely attack. Where collusion is required, the strength of function requirement is considered to have been met if the collusion can easily be detected and traced to its source by the use of the TOE's audit functions.

7.4.2 In assessing the strength requirements of cryptographic functions, the evaluators shall bear in mind that an attacker may be able to take a copy of some encrypted data and store it until improved crypto-analytic techniques become available. The personal data stored in the TOE could remain sensitive during the subject's entire lifetime, in the worst case 100 years from the time of data capture. Any key whose exposure would reveal the content of a substantial fraction of the database(s) must be capable of resisting attack for this period of time. Keys whose exposure would reveal only small fractions of the database(s) must resist attack for a shorter period, such as 30 years. Keys used for authentication only must resist the attacks which are possible at the time the protocol is run.

7.4.3 [Keys] may be used to estimate future crypto-analytic capabilities. Public-domain crypto-analytic capabilities should be reviewed regularly and frequently during the life of the TOE.

7.4.4 The following functions are seen as having a strength:

- a) cryptographic functions FCS\_\* (notwithstanding [CEM] Paragraph 424)
- b) authentication functions FIA\_\*
- c) statistical inference countermeasures specified in Section 6.5.

## 8 TOE Summary Specification

### 8.1 TOE Security Features

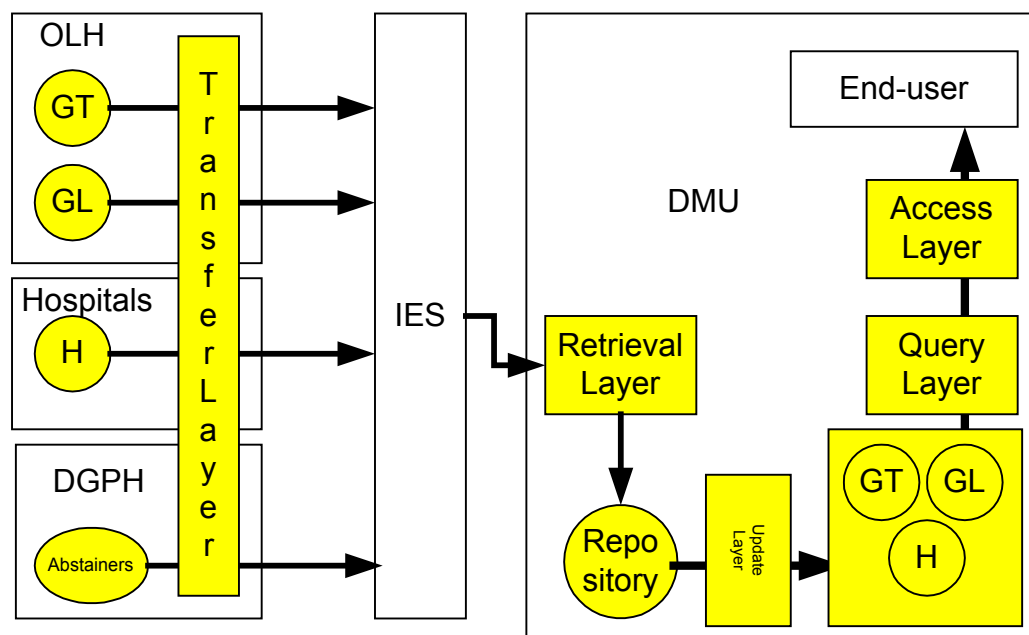
8.1.1 This section describes an early design for the TOE. It is included to aid in comprehension of the previous chapters. It is included for background information only. In the event of any conflict between the contents of this section and any other part of this ST, this section should be ignored.

8.1.2 The principal cryptographic keys used by the TOE are:

- a) the classification keys, one for each data type (GT, GL, H). These keys are used to encrypt identifiers in the data repository. The keys are symmetric.
- b) the transfer key. This is used to encrypt personal medical data so that the IES and database administrators cannot see it.

8.1.3 Each key has a key custodian who is responsible for its generation, storage, and input to the TOE.

8.1.4 The following diagram shows the high-level outline of components and data flows over the entire project.



8.1.5 The high level components of the TOE are:

- a) the Transfer Layer. This encrypts data sent to the IES. Two forms of encryption are performed:
  - i) SSL is used to encrypt data over the network to protect against eavesdropping
  - ii) the personal identifiers are hashed (i.e. one-way encrypted) so they cannot be decrypted
  - iii) the transfer public key is used to encrypt personal data using the IHD's public key so that it cannot be read by the IES
- b) the IES. One-way encryption is used to encrypt the hashed personal identifiers. Any incoming record whose ID appears in the abstainers list is removed here

- c) the Retrieval Layer. This encrypts the personal IDs again, using different classification keys for GL, GT and H data
- d) the Update Layer. This decrypts the health data (using the transfer private key) and further encrypts PNs (using classification keys controlled by the DPA). This ensures that cross-referencing via a direct access to the data stores (GL, GT, H) is impossible
- e) the Query Layer. This applies the inference controls and provides the only research capability in the system. The Query Layer is the only component where cross-referencing between the GL, GT and H data stores can take place
- f) the Access Layer. This authenticates the end-user and handles communications with him.

8.1.6 The high level data stores in the diagram (including some items not in the TOE) are:

- a) the GL and GT data within IE. This data is encrypted under the control of the DPA. Further procedural means are used to ensure that data and corresponding identifiers are never available to the same people.
- b) the H data in preparation in institutions. The health institution is responsible for ensuring that raw H data, along with all the other data maintained by the institution, is kept private.
- c) the abstainers list. This is a list of symmetrically encrypted hashed identifiers.
- d) the repository. This consists of medical data, encrypted using the transfer key, and identifiers, symmetrically encrypted and hashed and encrypted again (with different classification keys for GT, GL and H identifiers). Pre-processing is done at the repository
- e) the data warehouse. This consists of unencrypted H, GT and GL databases, accessible only by the Query Layer. The Query Layer holds the necessary keys to form a cross-reference between the three sets. The keys are controlled by the DPA.

## 8.2 Assurance Measures

8.2.1 The developer shall define a software and technology development process. This shall include:

- a) a development lifecycle for software
- b) a configuration and version management system
- c) test procedures
- d) defined responsibilities for development.

8.2.2 See Section 1.2 of [DDXD.002] for more information.

## 9 Rationale

### 9.1 Security Objectives Rationale

9.1.1 Table 9.1 provides a mapping between threats and security objectives to show that each of the threats is covered by at least one objective and that each objective meets at least one threat.

Table 9.1: Threats/Objectives Mapping		
Threats	Assets	Security Objectives and Assumptions
T_IMPERSONATE	All	OBT_AUTH, OBE_ACCOUNT
T_DIRECT	A_DHD	OBT_PROT, OBE_ROLE, ASS_SEPARATE, OBE_SUPERVISE
T_STATISTIC	A_DHD	OBT_PROT, OBE_ROLE, ASS_SEPARATE, OBE_QUERY
T_FILTER	A_DHD	OBT_AUDIT, OBT_AUTH, OBE_ACCOUNT, OBE_QUERY
T_COMMS	All	OBT_COMMS
T_AUDIT	All	OBT_AUDIT, OBE_ACCOUNT
T_ABSTAIN	A_IESDATA	OBT_ABSTAIN

9.1.2 OBE\_PHYSICAL, OBE\_PROCEDURE and OBE\_TRUST contribute to meeting all of the threats.

9.1.3 In most cases, the relationship between threats and objectives in Table 9.1 above is obvious. The following list clarifies some issues:

- a) T\_DIRECT and T\_STATISTIC - OBT\_PROT provides protection against authorised users, and OBE\_ROLE limits the number of authorised users. ASS\_SEPARATE provides protection in the information provider's environment
- b) T\_FILTER - OBT\_AUTH and OBE\_ACCOUNT ensure that only MCHSD/DPA/IEC members can authorise queries and OBT\_AUDIT ensures that they can be held accountable for what they have done. OBE\_QUERY requires query classes to be secure.

### 9.2 Security Requirements Rationale

9.2.1 Table 9.2 below shows that all the OBT\_\* security objectives are met by virtue of the IT functional requirements specified for the TOE.

9.2.2 Table 9.2 (and the following paragraph below) include all the IT functional requirements of this ST. Hence, in conjunction with Table 9.3 (see below), and with the notes in the following paragraphs, it may be concluded that the specified functional requirement components form a consistent and mutually supportive set.

9.2.3 The OBE\_\* security objectives are met by virtue of the environmental assurance requirements defined in Section 7.3.

<b>Table 9.2: Objectives/Requirements/Assumptions Mapping</b>	
<b>Security Objectives</b>	<b>IT Functional Requirements</b>
OBT_PROT	FCS_*, FDP_ACC.2, FDP_ACF.1, FDP_RIP.2, ST_GEN, ST_PERT, ST_QUERY_SIZE, ST_STATS, ST_SUBSET, ST_PN_CHANGE, ST_ATTR_EXCL, ST_ATTR_GRAN, ST_MIN_MULT, ST_NONDET, FAU_SAA.1, FAU_ARP.1, ST_AUDIT
OBT_AUTH	FIA_*, FTA_*, ST_FIRST_PW
OBT_ABSTAIN	ST_ABST
OBT_COMMS	FDP_ITT.*, FCS_*
OBT_AUDIT	FAU_*

9.2.4 The FMT\_\* and FPT\_\* requirements have not been mapped to a specific objective because they support all the objectives together. FCS\_\* supports the use of cryptography where needed.

9.2.5 OBT\_PROT is a complex objective and a detailed rationale is given below. Each type of threat agent is considered separately:

- a) information providers. These are responsible for the source data from which the IHD and the GLe and the GTe and the abstainers list are derived (see Table 6.1). Information providers are able to access the source data as they prepare information for transfer to the IES, but such access is outside the scope of this ST. ASS\_SEPARATE ensures that information providers are not able, as a result of the information preparation process, to relate personal identification data (e.g. name, address) to other data for any records for which they were unable to ascertain this relation prior to the information preparation process
- b) key custodians. These have access to cryptographic keys used to decrypt records. They do not have access to the encrypted or unencrypted records themselves because of role restrictions (FMT\_SMR.2, see also Table 6.1)
- c) access administrators. These can administer security but are not able to access any sensitive data themselves (see Table 6.1 and FMT\_SMR.2). The ST\_FIRST\_PW requirement prevents access administrators from impersonating users they have created
- d) operating system administrators. These are not given access to any unencrypted sensitive data (see Table 6.1 and FMT\_SMR.2)
- e) database administrators. These are not given access to any unencrypted sensitive data (see Table 6.1 and FMT\_SMR.2)
- f) hardware administrators. These are not given access to any sensitive data (see Table 6.1 and FMT\_SMR.2) and their access to the system is supervised (OBE\_SUPERVISE)
- g) IES normal users. These are not given access to any data (see Table 6.1)
- h) IES administrators. As with access administrators, these do not have access to any sensitive data themselves, and ST\_FIRST\_PW prevents them from impersonating users they have created

- i) members of the MCHSD/DPA/IEC. These do not get any access to TOE data (Table 6.1). They determine what query classes are permissible to an end-user or a customer. They have no means to attack the TOE directly, though they could assist an attack by an end-user or customer. The audit requirements (FAU\_GEN.1) ensure that such collusion is traceable to the perpetrator. The strength of function requirement excludes collusion between two TOE user classes. The MCHSD/DPA/IEC members have access to audit logs and ST\_AUDIT ensures that security cannot be compromised through this
- j) end-users. These do not have the capability to access IGG data directly; they have to submit requests for IGG data via the QL (see Tables 6.1-2). Countermeasures must safeguard privacy within the IHD and the GLe and the GTe against statistical inference attacks such as those described in Paragraph 4.2.3.3. An end-user may directly process 'his' IR data (derived from IGG data), but whatever processing he may perform on this IR data cannot yield new information that could allow him to infer private information. [ST\_GEN] and [ST\_PN\_CHANGE] (which can be supported by [ST\_NONDET]) prevent two end-users colluding to aggregate their respective IR datasets. Both administrative and technical SICs are required; they are regularly and frequently reviewed to take account of current best practice. Some potential attacks and their technical countermeasures are as follows:
  - i) tracker and linear system attacks - these may be countered by query subsetting [ST\_SUBSET], and by defining attributes' granularity and minimum multiplicity [ST\_ATTR\_GRAN] and [ST\_MIN\_MULT]); these SICs prevent attackers from isolating particular records
  - ii) median attacks - these may be countered by the exclusion of attributes [ST\_ATTR\_EXCL] that could lead to violation of an individual's privacy
  - iii) insertion and deletion attacks - these are not feasible because no end-user can insert or delete records at will (Table 6.1)
  - iv) diophantine attacks - these are countered by the minimum query size restriction [ST\_GEN] and [ST\_QUERY\_SIZE]; they may also be countered by the addition of noise [ST\_PERT], and the exclusion of attributes [ST\_ATTR\_EXCL] that would facilitate such an attack
  - v) averaging attacks - for a minimum query set size of 10, at least 150 queries (selecting an identical record set) must be made over a restricted query set to have any chance of gaining accurate enough data to perform a tracker attack [Denning, 6.5.2]. The audit and alarm requirements alert the administrators of such an attack [FAU\_SAA.1], [FAU\_ARP.1]
- k) customers. These do not have the capability to access the IHD or the GLe or the GTe, nor to access IR data directly; they have to submit requests for IR data via the RDL (see Tables 6.1-2). These requests are subject to the same SICs as may be deployed with respect to end-users' requests (see above); in particular, [ST\_GEN] and [ST\_STATS]) ensure that microdata is never returned to a customer
- l) pre-processor users. These have limited access to unencrypted data derived from the H database. They are given access to records one at a time and cannot choose the records they view. No personal identification data is included in what they can view (see Table 6.1). These users are healthcare professionals and can be expected to be trustworthy
- m) persons without legitimate access to the TOE. These should not be able to overcome the TOE's authentication functions (FIA\_\*) and physical protection measures, and so cannot access the TOE and its data.

## 9.2.6

FDP\_RIP.2 applies to protection against all types of users. It ensures that deleted or relocated data is not made available when data space is reallocated.

<b>Table 9.3: Requirements Components Dependencies</b>	
<b>Security Functional Requirements</b>	<b>Dependencies</b>
FAU_ARP.1 Security Alarms	FAU_SAA.1
FAU_GEN.1 Audit Data Generation	FPT_STM.1
FAU_GEN.2 User Identity Association	FAU_GEN.1, FIA_UID.1
FAU_SAA.1 Potential Violation Analysis	FAU_GEN.1
FAU_SAR.1 Security Audit Review	FAU_GEN.1
ST_AUDIT Audit Records Non-sensitive	FAU_GEN.1, FAU_SAR.2
FAU_SAR.2 Restricted Audit Review	FAU_SAR.1
FAU_SAR.3 Selectable Audit Review	FAU_SAR.1
FAU_SEL.1 Selective Audit	FAU_GEN.1, FMT_MTD.1
FAU_STG.1 Protected Audit Trail Storage	FAU_GEN.1
FAU_STG.4 Prevention of Audit Data Loss	FAU_STG.1
FCS_CKM.1 Cryptographic Key Generation	FCS_CKM.4, FMT_MSA.2, FCS_COP.1
FCS_CKM.2 Cryptographic Key Distribution	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.3 Cryptographic Key Access	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4 Cryptographic Key Destruction	FCS_CKM.1, FMT_MSA.2
FCS_COP.1 Cryptographic Operation	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.2 Complete Access Control	FDP_ACF.1
FDP_ACF.1 Security Attribute Based Access Control	FDP_ACC.1, FMT_MSA.3
FDP_ITT.1 Basic Internal Transfer Protection	FDP_ACC.1
FDP_ITT.3 Integrity Monitoring	FDP_ACC.1, FDP_ITT.1
FDP.RIP.2 Full Residual Information Protection	
ST_ABST Abstaining	FDP_ACF.1
ST_GEN General SIC Requirements	FDP_ACF.1
ST_PERT Data Perturbation	FDP_ACF.1
ST_QUERY_SIZE Query Set Size Restriction	FDP_ACF.1
ST_STATS Statistical Data Restriction	FDP_ACF.1
ST_SUBSET Operating on a Subset of the Database(s)	FDP_ACF.1
ST_PN_CHANGE Prevent Tracking of PNs in Different Sessions	FDP_ACF.1
ST_ATTR_EXCL Attribute Exclusion	FDP_ACF.1
ST_ATTR_GRAN Define Attribute Granularity	FDP_ACF.1
ST_MIN_MULT Define Minimum Multiplicity of Attributes	FDP_ACF.1
ST_NONDET Non-deterministic Choice of Records	FDP_ACF.1
FIA_AFL.1 Authentication Failure Handling	FIA_UAU.1
FIA_ATD.1 User Attribute Definition	
FIA_SOS.1 Verification of Secrets	
ST_FIRST_PW Confidentiality of Secrets	FIA_UAU.2, FIA_UAU.5, FIA_SOS.1, FMT_SMR.2
FIA_UAU.2 User Authentication before any Action	FIA_UID.1
FIA_UAU.4 Single-use Authentication Mechanisms	

<b>Table 9.3: Requirements Components Dependencies</b>	
<b>Security Functional Requirements</b>	<b>Dependencies</b>
FIA_UAU.5 Multiple Authentication Mechanisms	
FIA_UAU.7 Protected Authentication Feedback	FIA_UAU.1
FIA_UID.2 User Identification before any Action	
FIA_USB.1 User Subject Binding	FIA_ATD.1
FMT_MOF.1 Management of Security Functions Behaviour	FMT_SMR.1
FMT_MSA.1 Management of Security Attributes	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3 Static Attribute Initialisation	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1 Management of TSF Data	FMT_SMR.1
FMT_SAE.1 Time-limited Authorisation	FMT_SMR.1, FPT_STM.1
FMT_SMR.2 Restrictions on Security Roles	
FPT_AMT.1 Abstract Machine Testing	
(deleted)	
FPT_RVM.1 Non-bypassability of the TSP	
FPT_SEP.1 TSF Domain Separation	
FPT_STM.1 Reliable Time Stamps	
FPT_TST.1 TSF Testing	FPT_AMT.1
FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions	FIA_UID.1
FTA_SSL.1 TSF-initiated Session Locking	FIA_UAU.1
FTA_SSL.2 User-initiated Locking	FIA_UAU.1
FTA_TAB.1 Default TOE Access Banners	
FTA_TAH.1 TOE Access History	

9.2.7 Table 9.3 above lists the dependencies of the requirements components for the TOE (as specified in the CC for CC components). Most dependencies are satisfied by virtue of each specified component, or a stronger component from the same family, being within the TOE security (IT functional or IT assurance) requirements. The exceptions are displayed in bold face in the table and explained below:

- a) (deleted)
- b) FMT\_MSA.2 requires values input by administrators to be constrained to secure values. It is hard to see what such a requirement could mean; surely if the TOE knew what value was secure, it would not require input from the user. The requirement appears to be nonsensical, and has therefore been excluded. Note that the ADV\_MSU.1 assurance component ensures that users are given adequate guidance and the OBE\_TRUST objective ensures that users do not abuse their privileges.

9.2.8 The explicitly stated requirements (ST\_\*) have been included because the types of functionality required for statistical database security are not specified in [CC] Part 2.

### 9.3 TOE Assurance Level Rationale

9.3.1 The EAL3 set of assurance components is selected as the fundamental set for this ST, since this represents a reasonable compromise between:

- a) the desire to set a standard which has a reasonable chance of being achieved in a practical development

- b) the need for gaining an acceptable degree of assurance in the security of the TOE, given its potential for mishandling large amounts of sensitive data.

9.3.2 The augmentation (from AVA\_VLA.1 to AVA\_VLA.3) for statistical inference countermeasures was done because the original VLA level was not considered to provide sufficient assurance that statistical attacks had been properly dealt with. VLA.3 should provide adequate assurance, and is feasible given that statistical attacks rely upon externally visible functionality rather than internal design knowledge.

9.3.3 Note that the AVA\_VLA.3 component has dependencies on ADV\_IMP.1 and ADV\_LLD.1, which have not been included. This is considered acceptable because the statistical inference countermeasures can be adequately specified without meeting these requirements, and their security is not likely to depend upon the precise implementation used.

## **9.4 Environmental Assurance Level Rationale**

9.4.1 The assurance components chosen for the environment are roughly equivalent to EAL1. This is the highest assurance level that can sensibly be applied to a non-IT based system because the representations needed for higher assurance levels, such as high-level design, are only meaningful for an IT-based system.

9.4.2 The functional specification requirement (ADV\_FSP.1) has been changed to a requirement for a BS7799 style information security policy.

## **9.5 Strength of Function Rationale**

9.5.1 The strength of function requirement was chosen with regard to:

- a) the potential damage that people could suffer if sensitive information about them is disclosed
- b) the potential benefit that an attacker could gain from compromising the security of the TOE
- c) the availability of other methods of gaining sensitive information about an individual
- d) the requirement that it be impracticable to relate data in the IHD or the GLe or the GTe or the IR to a person's identity.