System-Level Security Policy (SLSP)

1. System Details

1.1. The system shall be known as: Cancer Survival Group.

1.2. The system's responsible owner shall be Professor Michel P Coleman.

1.3. The system's Caldicott Guardian shall be the Director of Resources and Planning from the London School of Hygiene and Tropical Medicine (LSHTM).

2. Introduction and Purpose

2.1. The Cancer Survival Group (CSG) processes sensitive patient data for the purposes of its programme of research as a secondary user of those data.

2.2. The purpose of this SLSP is to serve as an Information Governance policy, to safeguard the confidentiality and security of the sensitive patient data held by the Cancer Survival Group.

2.3. All original sensitive identifiable patient data are stored and processed in a secure environment (the Secure Annex).

2.4. Sensitive but de-identified data may be exported to the LSHTM network, on which the analyses are produced, protected by username and password and the appropriate file system access rights.

2.5. "Sensitive personal data" (Data Protection Act (1998 c29), Part I, Section 2[1]), held by the Cancer Survival Group are personal data relating to a person's physical or mental health or condition, to the diagnosis of his condition or to his care or treatment, where "condition" refers specifically to a malignancy registrable under the NHS Act (2006 c41, Section 251) and the Health Service (Control of Patient Information) Regulations 2002 (SI/2002/1438, Section 2).

3. System Security

3.1. Security of the system shall be governed by the LSHTM Information Management and Security Policy.

3.2. The System's responsible Security Manager shall be Professor Coleman.

3.3. The security manager's duties shall include overseeing the creation of appropriate storage areas with the appropriate security rights, and ensuring that staff granted access are aware of their responsibilities in relation to information security. The duties shall also include nomination of a CSG staff member as the Information Governance Lead.

3.4. The Information Governance Lead shall be Adrian Turculeţ.

3.5. The responsibilities of the Information Governance Lead shall include coordinating, publicising and monitoring standards of information handling within the Cancer Survival Group; developing and implementing an information governance improvement plan, and

[1] http://www.legislation.gov.uk/ukpga/1998/29/section/2

ensuring that the requirements for information governance assessment are submitted on schedule and in the required form to the relevant authority.

3.6. In the absence of the Information Governance Lead, a senior academic staff member (Professor or Associate Professor) of the CSG may deputise for the Information Governance Lead to approve a data transfer.

3.7. The system has been created to protect sensitive data in a manner that follows the guidance on information security management practice set out in BS ISO/IEC 27002:2013.

Physical access to LSHTM and to the Secure Annex

3.8. Access to the London School's main building in Keppel Street requires electronic logging of a valid personal photo-identity card issued only to LSHTM staff members. The entrance is monitored by in-house staff during working hours and by contracted security staff at other times. Staff must sign an entrance log if they do not have their ID card.

3.9. Monitored, video surveillance of the entrance and other parts of the building is in operation 24 hours a day, 365 days a year. Security personnel make frequent rounds to all parts of the building, both day and night, during which they check doors and log in to data points around the building.

3.10. Access to the research areas of LSHTM requires passage through security doors using the personalised magnetic security and ID card.

3.11. Room 254 is a large office accommodating staff of the Cancer Survival Group and no other staff. Room 253 is an adjoining room forming part of this office, accessible only via Room 254. The door to Room 254 is manually locked whenever the room is empty, in other words by whoever leaves the room empty, even for a few minutes, whether that is during normal working hours, during fire alerts or at any other time. Each CSG staff member has a key to Room 254 and is required to report loss of that key at once.

3.12. The sensitive data held by the Cancer Survival Group are stored on secure stand-alone computers in the Secure Annex. The Secure Annex is a small, windowless room, entirely contained within Room 253. It can only be accessed from Room 253, through a self-locking door that requires entry of a digital security code on a keypad. The security code is changed by the Information Governance Lead every three months, or immediately after the departure from employment of any authorised person (see below), whichever is sooner. The code is communicated only to authorised persons.

Persons authorised to enter the Secure Annex

3.13. Access to the Secure Annex is restricted to named individuals ("authorised persons"). Authorised persons must first have signed the Cancer Survival Group's confidentiality declaration that they understand and accept the conditions for access and will abide by them. The list of authorised persons and the originals of their signed confidentiality declarations are maintained and updated by the Information Governance Lead or Security Manager.

3.14. Any proposed addition to the list of authorised persons must be agreed by the Information Governance Lead, who will provide an induction into information governance and obtain a signed confidentiality declaration. The induction takes the form of a face-to-face discussion of the principles of data security and of the procedures operated by the Cancer Survival Group to maintain the physical and electronic security of individual data.

3.15. Cancer Survival Group personnel must also complete the London School of Hygiene and Tropical Medicine's *Information Security Awareness* training before they can be designated as an authorised person and given the access code to the Secure Annex.

3.16. When an authorised person is working on sensitive data in the Secure Annex, only other authorised persons may be present. When an authorised person in the Secure Annex leaves the room empty, s/he must ensure that the door is closed and locked, requiring re-entry of the code to gain access, even if the Secure Annex will only be empty for a few moments.

4. System Management

4.1. This security system was developed by the Cancer Survival Group at LSHTM, in consultation with the Head of Information Technology at LSHTM.

4.2. The system is implemented by the Cancer Survival Group. No external contractor is involved. Should a secure computer require repair, that repair must be accomplished by LSHTM IT staff, without moving the computer, and under the direct observation of an authorised person. If a secure computer is irreparable under those constraints, the hard disk must be wiped electronically, then removed and physically destroyed by Cancer Survival Group staff. The backup systems must then be used to load a new secure computer.

4.3. The secure computer system is not shared with any other research group or institution.

5. System Design

5.1. Sensitive data are stored in the Secure Annex, and only there, on non-networked computers (secure computers). The secure computers are not attached to the internet, or to the LSHTM intranet, or to any wireless network. The secure computers do not have wireless capability. The stored data are thus not remotely accessible. Apart from the external hard drives designated and labelled specifically for download, backup and transfer, respectively, no other electronic device (desktop, laptop, PDA, flash drive) is permitted in the Secure Annex, regardless of whether that device has wireless capability.

5.2. Separate, external hard drives are used: (a) for download of encrypted data files sent by data suppliers, (b) for backup, (c) for transfer of anonymised data from the secure computers to the network computers used for data analysis, and (d) for transfer of files that do not contain individual patient data, e.g. text files containing lists of NHS geographic areas. The hard drives are clearly labelled Download, Backup, Transfer and Non-confidential transfer. Use of each external hard drive is absolutely restricted to its designated purpose. The external hard drives used for backing up sensitive data are all encrypted.

5.3. A fireproof safe located in the Secure Annex is used to store all the external hard drives when they are not actually in use. Original CDs or DVDs of sensitive, potentially identifiable data are also kept in the safe.

5.4. There is only one key to the safe. The safe key is locked in a safe-box, outside the Secure Annex, under control of the Information Governance Lead, at all times when not in use.

5.5. The secure computers were bought and installed specifically for the storage and manipulation of confidential data. They are accessible only under strictly controlled circumstances.

5.6. Access to the data stored on the secure computers is restricted to authorised persons in the Cancer Survival Group. Access to the computers is controlled by the appropriate assigned

rights and by password. The password is regularly modified by the Information Goverance Lead.

5.7. No printer is allowed in the Secure Annex.

6. Operational Processes

6.1. Sensitive data are transmitted to the Cancer Survival Group via one of two methods.

6.2. The first method is the CONCORD File Transmission Utility, developed to support the CONCORD programme for the global surveillance of cancer survival. The CONCORD programme receives individual cancer patient data from several hundred population-based cancer registries world-wide, under statutory and ethical approval within the UK (ECC 3-04(i)/2011, 11/LO/0331) and from participating jurisdictions in more than 70 countries. The utility is described in Annex 3 to the CONCORD-3 protocol. The utility transmits password-protected files. It deploys 256-bit Advanced Encryption Standard (AES-256) security for envelope-encryption of files being transmitted. Data files are protected by one-time, random, "strong" passwords that are automatically generated at the moment of data transmission. These passwords are not stored, but sent separately to the Cancer Survival Group.

6.3. The second method is special courier delivery. Not all collaborating research institutions have secure and reliable access to the internet. Some institutions that do have such access prefer courier delivery, judging it more secure than electronic methods. Receipt of courier deliveries must be acknowledged by signature in person of an LSHTM staff member. Delivery must also be separately confirmed to the data supplier by the courier company.

6.4. Data transmitted via courier may be stored on any standard storage device (CD or DVD preferred). The data files must be protected with advanced encryption (e.g. using the latest versions of WinZip or 7-Zip) and a strong password. Before sending a data transmission by courier, the data supplier must first send an email describing the content of the package, and providing the following details: name and address of the data supplier, details of the courier company, date of transmission, the physical contents of the package, and the name and email address of the data supplier to whom receipt should be notified. The data supplier must also provide a contact number from which the password can be obtained. The CSG member of staff dealing with the data must document these details in the Secure Annex log book.

6.5. Any email that may be received that includes attached individual data, which should not have been sent in this way, must be immediately and permanently deleted. Any such emails must be deleted before the regular end-of-month backup, which is performed on the last Friday evening of each month. The sender of the data must also be informed, so that the mistake is not repeated.

6.6. Sensitive data are stored in electronic format, only, on the system's secure computers (as described above). Sensitive data received from data suppliers, whether on CD or DVD, or via the CONCORD File Transmission Utility, are immediately transferred to one of the secure computers. Original CDs and DVDs are stored in the safe. The Download hard drive is then wiped, and stored in the safe.

6.7. All sensitive data are either encrypted or stored in the Secure Annex, either on one of the secure computers or in the safe.

6.8. Back-ups of the secure computers' hard disks are made regularly.

6.9. Any anonymised data extracts that need to be copied from the secure computers to the LSHTM network must be approved by the Information Governance Lead. A form containing the name of the requestor, name of the file extract, date, variables included in the extract and the identifiable variables that have been stripped is sent to the Information Governance Lead, who must approve the transfer and generate a security code. If the Information Governance Lead is not available, the transfer must first be approved by a senior academic member of the CSG (section 3.6). The date, time and security code of any data transfer must be written in the Secure Annex log book, signed by the person who made the transfer.

6.10. Data sets that have been anonymised and transferred from the secure PCs to the LSHTM network may be accessed from a high-powered, secure server that is hosted in the LSHTM data centre. This server allows analyses to be performed more quickly than with regular desktop computers. The server is owned by the Cancer Survival Group and is accessible only to CSG staff who have been granted access by the Information Governance Lead.

6.11. Unattended PCs should be manually or automatically secured by locking them with a password-protected screen saver.

7. Disposal of identifiable electronic data

7.1. Some collaborating agencies request destruction of their data after completion of the study. We comply, and we document this. When the data are no longer needed, data files are shredded using proprietary software that overwrites purged disc blocks with random patterns of characters (up to seven sequential data shred patterns may be placed over deleted data), making them completely unrecoverable. We use the Eraser software described in the National Industrial Security Program Operating Manual of the US Department of Defense (http://eraser.heidi.ie/trac). Any related CDs or DVDs are physically destroyed.

8. System Audit

8.1. The system will be periodically risk-assessed by LSHTM IT managers. Any unacceptable risks will be immediately addressed by the Cancer Survival Group and the actions subjected to further evaluation by LSHTM IT staff. Any material change to the physical and electronic security arrangements covered in this SLSP will be notified to the relevant statutory authority, currently the Confidentiality Advisory Group of the Health Research Authority, so that any additional security review deemed necessary may be carried out.

9. System Protection

9.1. Resilience is provided by the standard backup procedures outlined above. Original data are retained on the source CD or DVD, the secure computers and the external backup drives. Modifications are backed up. In the event of failure of either a secure computer or a backup drive, the failed component must be securely wiped, physically destroyed and replaced, and the data stored on the replacement component.

9.2. In the event of a breach of physical or electronic security, or of confidentiality, we would (a) immediately assess the nature, the extent and the cause of the breach; (b) inform the Caldicott Guardian of LSHTM (the Secretary and Registrar); (c) notify the data supplier in the form and on the timescale specified in the agreement for data supply; and (d) take whatever other steps may be deemed appropriate to secure all other data, recover the data lost and minimise the impact of the loss of data.

10. Ownership of the System Level Security Policy

10.1. This System Level Security Policy is the responsibility of Professor Michel P Coleman. It is reviewed annually or more frequently if required for completeness, relevance and any necessary updates, in collaboration with Cancer Survival Group staff and LSHTM IT staff.

10.2. This System Level Security Policy has been distributed to Cancer Survival Group staff, LSHTM IT staff and the Confidentiality Advisory Group of the Health Research Authority.

11. Data Protection Registration

11.1. LSHTM is registered under the Data Protection Act 1998 (1998 c29). The registration (Z7513362) covers the classes of data held by the Cancer Survival Group and the purposes of analysis for which those data are used.

Dr Michel P Coleman BA BM BCh MSc FFPH

Professor of Epidemiology and Vital Statistics
Cancer Survival Group
Department of Non-Communicable Disease Epidemiology
London School of Hygiene and Tropical Medicine
Keppel Street
GB-London WC1E 7HT
T +44 20 7927 2551
michel.coleman@lshtm.ac.uk