N. Ireland Cancer Registry

Policy Regarding Security, Confidentiality and Issue of Data

Located in:

Centre for Public Health

Updated August 2015

Contents

These Guidelines have been submitted to the Steering Group of the NICR, the Council of the Registry and The Office of Research Ethics NI (2010). They will be reviewed regularly by the Registry.

Data Protection Registration Number (QUB): Z6833827

The procedures outlined will be reviewed in the light of practice and up-dated as necessary.

<u>History of Updates</u>

Updated July 2015
Previously updated August 2014, September 2011, September 2010, March 2010, January 2008, March 2007 and January 2003

1. Introduction

1.1 This document contains guidelines for the handling and release of confidential data held by the N. Ireland Cancer Registry. It updates the previous Cancer Registry documents.

1.2 The N. Ireland Cancer Registry (NICR) was established in May 1994. Its role is to establish and run a computerised information system on cancers diagnosed in the Northern Ireland population for the purposes of research, education and the planning of services (see appendix A for Aim & Objectives). In addition to information on cancers received after this date, the Registry has inherited, from the Department of Health and Social Services, data on registrations and deaths of cancer patients in Northern Ireland from 1959-1992. The number of new cancers registered in the old system was incomplete at approximately 5,000 per year. Currently 10,000 cancers are registered annually including approximately 3,000 skin cancers. The registry is the subject of an annual funding agreement between the Public Health Agency (PHA) and Queen's University of Belfast (QUB) with the option of regular reviews to ensure quality and to advise on direction. It is located within Queen's University Belfast in secure accommodation, on the Royal Victoria Hospital site. The Registry has a Steering Group and Council (see appendix B and C for role and membership).

1.3 The Agreement between the PHA and QUB sets out the terms by which the University contracts to maintain and operate the N. Ireland Cancer Registry.

1.4 The role of the Registry requires that there is a high level of data detail and quality to ensure accuracy. This is achieved by a multilevel quality assurance programme which matches data from many sources and identifies duplicate records.

1.5 In order to identify matched records the Registry requires patient identifiable data.

1.6 This document takes cognisance of the following documents.

a) The Data Protection Act 1998.
b) The General Medical Council (GMC) Guidance on Confidentiality (See Appendix D).
c) The UK Association of Cancer Registries Guidelines (latterly updated to UK and Ireland Association of Cancer Registries (UKIACR).
d) Queens' University Belfast, Data Protection Policy.

1.7 These Acts and Guidance have been instrumental in helping us all to think deeply about data protection and confidentiality of patient data. The N. Ireland Cancer Registry hosted a conference on this issue on 25 October 2001.

In Northern Ireland there is a Privacy Advisory Committee and NICR staff have made representation to them on the work of the registry and the need for a legislative framework for Northern Ireland. The need for a legislative framework was reiterated in the report of the Peer Review of the NICR in November 2007. A public consultation on the secondary uses of patient information has been completed and a bill on health and social care control of data processing is being prepared.

1.8 "Personal Data" means data consisting of information which related to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual.

1.9 The Information Commissioner, has added the following guidance:

"*A living individual*". For Cancer Registration purposes, the standard of confidentiality that applies to people living with cancer also applies to those who have died from the disease, except where specific exceptions exist as in the case of genetic counselling.

"Can be identified". The identification may be direct, e.g. where the subject's name is recorded as part of the data – or indirect, e.g. where the data contain a code from which, by reference to a separate list, the subject can be identified.

On disclosing, the Information Commissioner has also stated that:

a) there is no disclosure if the identification of the subject (of the personal data) is dependent partly on other information in the possession of the Data User which is not itself disclosed. The same point applies to transfers; and

b) the medium of disclosure is not limited, for example, it could be oral or hand-written as well as printed or displayed on a screen.

2. Guidelines on Confidentiality for Staff Working in the N. Ireland Cancer Registry

2.1 Some, but not all, staff in the N. Ireland Cancer Registry (NICR) will, in the course of their work, handle personal data on patients with a diagnosis of cancer. It is recognised that a name will directly identify a person but a person can sometimes be identified indirectly, for example, by an identification number, by their address etc. All personal data are regarded as confidential. Data may be in the form of hand-written, typewritten, microfiche, printed records or on machine-readable format.

2.2 The following data are considered to be those which may identify an individual:

Alone 1-6

1 Name(s) of registered person
2 Address of registered person
3 Case note number/histology number
4 Health and Social Care Number (HCN)/CHI number/Breast Screening Unit Patient Number
5 Postcode (in some instances)

In Combination 7-10

6 Date of Birth
7 Postcode of registered person
8 Consultant (Name or Code)
9 GP (Name or Code)

2.3 The Data Protection Act 1998 legislated on the fair obtaining, processing, storing and disclosure of data held on computer, paper or in machine form. A list of the principles of the Act is included in Appendix E.

2.4 The term "Confidential Information" applies to any data relating to identifiable individual patients, staff, practitioners or health care providers held on a document, microfiche or magnetic media. It should be noted that this may also apply to anonymised data (see below).

2.5 There are instances where non-personal data could be classified as "Confidential Information" or "Potentially Confidential Information" e.g. small numbers of rare cancers in areas of low population. For example cases of Kaposi's sarcoma, which can be directly related to HIV disease. Direction on when non-personal data becomes confidential or potentially confidential information is available from the Director of the NICR. It should never be assumed that aggregated data are not confidential information.

2.6 Confidentiality of data within the N. Ireland Cancer Registry is maintained by careful procedures to maintain:

a) The Physical Environment

The NICR while operating a local area network is separate from all other computer systems. The NICR is located within a secure section of Queens University of Belfast with enhanced security. The NICR is accessed through doors that have combination locks with regular changes to codes. It also has video surveillance. Identifiable data is held within an extra secure subsection of the Registry and accessed only via passwords and bioinformation.

b) Staff Understanding of Confidentiality Issues

Staff have had, and will continue to have, in-house training on issues of confidentiality. These will provide them with opportunities to consider specific cases and learn together as a team.

c) Procedures

i. The authorised users of the system are authenticated via their fingerprints.

ii. Transfer/transport of information will continually be reviewed. It is kept to a minimum and transported only with encryption if electronic.

iii. The training component of the NICR computer system contains fictitious data.

2.7 Staff Practices

Security of NICR premises:

a) All windows and doors must be secured at night and during prolonged absence from the room.

b) All visitors must be accompanied while on the premises, and a record kept of all visitors using the facilities of the NICR. Anyone not employed directly by the NICR should have and wear a visitor badge at all times.

c) The lock combination of the entrance door should be changed at least quarterly.

d) Room access for system support purposes will only be available during normal working hours and when Registry staff are present.

e) Access for cleaners will only be provided when NICR staff are present in the Registry.

2.8 It is important to maintain confidentiality while working with data.

a) Never examine or handle in any way personal data, except in the course of your work.

b) If you are required to read personal data as part of your work, these must never be disclosed to any person not directly concerned with that work.

c) It is each staff member's responsibility to ensure that the data they are working on are not read or handled by anyone who has no reason to do so. If you believe that someone is deliberately attempting to read

or handle personal data not within their official duties, the facts must be reported immediately to your supervisor or the Director of the NICR.

d) If you are working with personal data and you have to leave the room you must either lock the data away or ask another member to be responsible for the data until you return. Screensavers should be activated if working on computer.

e) If you are the only member left in charge of personal data and you have to leave, the data must be locked away and the room locked. Screensavers should be activated if working on computer.

f) Photocopies of confidential documents should only rarely be required to be made and in such cases the approval of the NICR Director is necessary.

g) Staff must always "log out" of their terminal/PCs when leaving the building, leaving the office to attend meetings, leaving the office empty, or when the office will be occupied solely by non-NICR staff/visitors.

h) Person identifiable data must never be left visible on an unattended terminal/PC screen.

i) Confidential information may only be destroyed by methods applicable to confidential waste, for example, shredding.

j) Where possible no individual identifiable data should be given over the telephone. If this is unavoidable, this must be done by returning the enquirer's call after checking the validity of the number and caller.

2.9 While Not Working with Data

Confidential information must never be left unlocked in an unattended room, it must be kept in secure locked cupboards or cabinets when not in use, and must not be taken out of the NICR premises except as specified below. Staff must not hold personal data from the NICR on a home computer. Neither is it permitted for staff to take home magnetic media and printouts holding personal data. These may only be removed from the office if required, for example, in connection with validation visits to hospitals. Such data must be kept in a secure container.

a) If it is discovered or even suspected that confidential information has been lost, your supervisor must be informed immediately. He/she must investigate and report to the NICR Director without delay.

b) Keys to cupboards holding confidential information must be locked away or kept on the person when not in use. The Registry Office has a coded lock, the combination of which is regularly changed.

2.10 Transport of Data

Confidential information must be transported by a secure method, whether it is on paper or electronic media. In all methods of posting confidential information to a third party in paper format confidential material should be enclosed and sealed, double wrapped, in a tamper proof envelope or container. Transit envelopes should not be used. All data leaving the office to be marked **"PRIVATE & CONFIDENTIAL"** and addressed to a named person.

a) Confidential information should be sent via HSCNI email when appropriate. For standard transfers to hscni.net email accounts, should be carried out by a member of Registry staff who has an hscni.net email account. Electronic data should be encrypted and password protected to ensure security and confidentiality. The password should be sent separately and only after the verified contact acknowledges the safe reception of the data. Randomised passwords employing at least 20 characters (mix of upper case, lower case, numbers, and symbols) must be used in the encryption process. In all electronic data transfers, 256-bit encryption tools should be employed for the encryption process, such as 7-Zip, WinZip (Version 9 and above) and TrueCrypt.

b) For exchange of information to an nhs.net email address (organisations outside of HSCNI but part of the NHS network in England and Wales), an nhs.net email account has been created (colinfox@nhs.net). This is a web-based facility (URL: https://web.nhs.net) and removes the need to encrypt files prior to transport. This is the only method available to transport data to recipients with nhs.net email addresses (such as cancer registries and health trusts in England and Wales). Data files requiring transfer should be given to either the IT Manager or the Data Manager who will be able to send them using this facility.

c) For the transport of confidential data to organisations outside the HSCNI network, the HSCNI encrypted mail procedure should be used – this procedure is outlined in Appendix I. With this facility, there is no requirement to encrypt the data files prior to transport. Of course, if preferred and to ensure desktop security, the files can be encrypted prior to transport.

2.11 Confidential data must be stored in a secure manner

a) All cancer-input data are held in, lockable cabinets/drawers. No data can be removed from these storage areas without the Director's approval.

b) All patient identifiable data including data on encrypted removable storage devices must be placed in lockable drawers/cabinets at close of day or during the day when the office is vacant. All such data must be cleared from desks when offices are empty.

c) Two back-up copies of the NICR database will be kept. One within the NICR and the other in a secure area outside of the Registry in central QUB safe facility. The Systems Manager will ensure that both copies are up-to-date and secure.

2.12 While working with computers

a) All passwords for data input, computer operations or access to data held on PCs must be changed quarterly or when there is a possibility that a breach of security has occurred.

b) Where possible named data should not be held on the hard disks of individual PCs but rather held/stored on the NICR system residing on the server machine.

c) Screen savers will be activated after ten minutes and user should manually activate the screen saver if a visitor enters a room. Screen savers may be de-activated by fingerprint on the internal NICR Network and by passwords o. The same security procedures apply to the laptop computers as other machines. A check will be made quarterly by the System Manager to ensure there is no unnecessary data on the machines.

2.13 Confidentiality Declaration

All staff working in, or on behalf of, the NICR are expected to sign an undertaking regarding confidentiality on their appointment. (Appendix F).

3. Release of Data

3.1 The intention of this code of practice is firstly, to ensure that no harm or distress should ensue for the individual patient or their family, and secondly to ensure that the doctor/patient relationship should in no way be impaired.

3.2 Only the Director of the NICR has the authority to release cancer data. The Director may delegate the release of data to other staff, but the responsibility for the release of data and that the correct procedures have been followed lies with the Director.

3.3 The NICR provides epidemiological information on cancers upon request. Reports on cancer deaths and cancer incidence have been widely circulated and are available on the web at www.qub.ac.uk/nicr. The NICR processes over 200 requests for information annually. Some relate to historical data, which is recorded on the old cancer registry system. Requests for information are usually performed by the Biostatisticians and release is authorised by the NICR Director. The release of information is subject to procedures as outlined in section 4.

3.4 We welcome information requests for research, education and planning purposes and the Registry will endeavour to process requests in as timely a fashion as possible subject to resources. Enquiries should be addressed in the first instance to the Director of the N. Ireland Cancer Registry. We will do our best to meet your information requests, subject to data availability and the requirements of this protocol. **Please take special note of any advice issued with regard to the adequacy or correctness of the data information we supply.**

3.5 If the information is used in any publication or official document, the NICR must be acknowledged as the source of the information. Unless we have participated in the finished report, it must state that the responsibility for interpretation of the data/information we supplied is the author's alone. Advance notification to the Registry of any findings based on cancer registry data that you intend to publish is required. The Registry's funding by PHA should also be acknowledged.

3.6 The requirements for the release of information differ according to whether or not the information would permit the identification of individual patients. It is the NICR's policy to treat information on named deceased patients under the same restrictions as those for living patients (except for genetic enquiries – *see paragraph 4.6*). See paragraph 2.2 for list of items considered to be those which may identify an individual.

For the most part, aggregated data will not be patient identifiable. In certain circumstances however, it may be possible to identify individual patients e.g. where it concerns rare tumours in sparsely populated areas. If it is the opinion of the Director that such aggregated data would permit the identification of individuals, applicants must fulfil the same requirements as for the release of identifiable data or suppress the small number.

4. Release of Data from the N. Ireland Cancer Registry

4.1 Research not requiring access to identifying individuals will be released following compliance with Standard Operating Procedure QUB-AD-NICR-002 (aggregate statistical data).

Where possible requests for other than routine data should be made, in writing, stating the purpose and method of the study using Request Form (Appendix G). The Declaration part of Form I must be completed and returned to the Registry by the applicant prior to the release of the data. If these requests are for a major research project or will require a major investment of time by Cancer Registry staff then the research proposal will be considered at the N. Ireland Cancer Registry with feedback of decision within two weeks.

4.2 Researchers requiring access to information potentially identifying individuals must complete Form I and Form IV (Appendix G).

4.3 Research requiring access to personal health records of patients:

a) The individual patient records held by the N. Ireland Cancer Registry are subject to a confidentiality undertaking between the clinician(s) in charge of the patient at the time of registration and the NICR and therefore clinicians may request information on their own patients Forms I and II (Appendix G) to be completed. If access is required by a researcher other than the treating clinician then, the approval of the treating consultant(s) must be obtained by the applicant before the research commences. This requires completion of Forms I, II and III (Appendix G). Where consultants' permission cannot be sought - e.g. consultant is unknown - the MDT Chair will be contacted.

b) If the applicant is not medically qualified, they must obtain a further signature from a medically qualified colleague who will be responsible for the confidentiality of the information supplied. The NICR will then provide a list of consultant(s) clinically responsible for the data. The applicant must then seek completion of Form III (Appendix G) by each clinician involved. Only then will the NICR release the data to the request applicant.

c) If the research involves contacting the patient this must be done with eligibility confirmed by patient's clinicians i.e. Consultant or GP prior to patient contact. Invitation letters to patients should have a return address and "To be opened by addressee only" on the outside of the envelope.

d) Where Ethical Committee approval is required, an approach must be made to the relevant Ethical Committee. Once approval has been given, written confirmation of this must be sent to the NICR. The NICR Director would be pleased to advise if Ethical Committee approval is required.

e) The data provided by NICR can only be used for the research purposes specified, and it must be impossible to identify any individual patient record in reports of the research.

f) All reasonable precautions must be taken to ensure that the personal information does not fall into unauthorised hands. All copies of the information must be destroyed by a date specified by the Registry when the research is finished or abandoned. The Registry will offer practical guidance to applicants on dealing with the disposal of information.

g) If data are transported to other locations, the rules set out in *paragraph 2.10* must be complied with. Transfer of data from outside the UK or Republic of Ireland must not be made without the authorisation of the Director. Such authorisation will generally only be given in respect of transfers to countries that are signatories of the European Convention of Data Protection or have been designated by EEC as meeting safe harbour privacy principles.

4.4 All identifiable data issued from the NICR (paper or electronic)

a) Must be accompanied by a letter quoting the number of pages in the report or disk number. Replies to information requests will be recorded indicating source of request and action taken. Electronic data release should be encrypted and password protected to ensure security and confidentiality. Randomised passwords employing at least 20 characters (mix of upper case, lower case, numbers, and symbols) must be used in the encryption process. The password should be sent separately and only after the verified contact acknowledges the safe reception of the disk.

b) The letter/package must be clearly marked **"PRIVATE & CONFIDENTIAL"** and sent to a named person when issuing patient identifiable information. In all methods of posting confidential information to a third party confidential information should be enclosed and sealed, double wrapped, in a tamper proof envelope or container.

4.5 Records of Information Requests.

All information requests will be held by the Data Manager. Once dealt with, completed NICR Request for Information Forms will be lodged with the Data Manager.

4.6 Genetic Counselling

The NICR provide data for clinical genetic counselling services to help verify suspected familial cancers. Information required for this service will be released to the appropriate medical practitioner in line with the

policy of the UKIACR ie **information on deceased patients is provided on request while information on live patients is provided only with evidence of written consent.** (Appendix G Form V)

4.7 Where people normally reside outside Northern Ireland and are registered with the N. Ireland Cancer Registry, the Registry undertakes to notify the registry covering the patient's area of residence. This is a reciprocal arrangement with other registries in the UK and Eire.

4.8 Examples of data requests are given in Appendix H.

APPENDIX A – N. Ireland Cancer Registry Aims and Objectives

The aim of the N. Ireland Cancer Register is to provide accurate, timely information on cancers occurring in the population of Northern Ireland for research, planning and education so that the burden of disease may be reduced and the experience of patients and their outcomes improved.

The objectives of NICR are to:

a. Collect and confidentially store accurate, timely and comprehensive data on cancers and pre-malignant disease occurring in the Northern Ireland population.
b. Uphold patient and carer confidentiality.
c. Analyse data to provide for the Registry's role as provider of official cancer incidence, prevalence and survival statistics for Northern Ireland.
d. Provide appropriate information on cancer for ad hoc queries.
e. Undertake and assist audits of cancer treatments, services and outcomes, and recommend improvements in cancer services where appropriate.
f. Facilitate planning of cancer services for prevention, diagnosis, cure and care.
g. Promote, facilitate and undertake research into cancer causes, prevention, treatments and outcomes.
h. Publish scientific reports and papers relating to cancer.
i. Promote professional and public awareness about cancer.
j. Link nationally and internationally to promote cancer registration and increase understanding and control of cancer.

Taken from 5-Year Strategic Plan April 2013

APPENDIX B – N. Ireland Cancer Registry Steering Group

Role: *The Steering Group has been appointed to oversee the work of the N. Ireland Cancer Registry including the approval of the annual budget.* **Frequency of meetings normally 3-5 times per year.**

MEMBERSHIP LIST:

Chair

- Dr David Stewart, Regulation and Quality Improvement Authority

Cancer Network Lead Clinician

- Dr Gerry Hanna, Consultant in Clinical Oncology, The northern Ireland Cancer Centre, Belfast City Hospital
- Dr Martin Eatock, Medical Director, Northern Ireland Cancer Network (NICaN)

User Representative

- Ms Roisin Foster, Cancer Focus Northern Ireland

University

- Professor Ken Mills, Centre for Cancer Research and Cell Biology
- Professor Liam Murray, Clinical Professor of Cancer Epidemiology, Acting Director of Centre for Public Health

Public Health Agency

- Dr Miriam McCarthy

Health & Social Care Board

- Sara Groogan, Performance Management and Service Improvement Directorate
- Lyn Benson, Financial Accounts and Governance

Director of N. Ireland Cancer Registry

- Dr Anna Gavin

Updated July 2015

APPENDIX C – N. Ireland Cancer Registry Council Group

Role "***to pursue the aims of the Registry and to identify and enhance opportunities for use of the Registry data***" by advising the Director and Steering Group. Frequency of meetings at least annually. It provides a mechanism to liaise with key stakeholders.

MEMBERSHIP LIST:

Surgery, Belfast Trust	- *Professor Roy Spence (Chair)*
Pathology, Belfast Trust	- *Dr Neil Anderson*
Lead Clinician, Northern Trust	- *Dr Jim Carson*
Lead Clinician, Southern Trust	- *Dr Rory Convery*
Dermatology, Belfast Trust	- *Dr Olivia Dolan*
Lay Representative	- *Dr Andrew Galwey*
Director, NICR	- *Dr Anna Gavin*
Health & Social Care Board	- *Ms Sara Groogan*
Northern Ireland Biobank	- *Dr Jackie James*
Lay Representative, NHSS Council	- *Professor George Kernohan*
Action Cancer	- *Mr Gareth Kirk*
General Manager, Cancer Services, Belfast Trust	- *Ms Davinia Lee*
Oncology, Belfast Trust	- *Dr Seamus McAleer*
Public Health Agency	- *Dr Miriam McCarthy*
Thoracic Surgeon, Belfast Trust	- *Mr Jim McGuigan*
Oncologist, Belfast Trust	- *Dr Sarah McKenna*
Macmillan Cancer Support	- *Ms Heather Monteverde*
Surgery, South Eastern Trust	- *Mr John Moorehead*
Clinical Professor of Cancer Epidemiology, Acting Director of Centre for Public Health, QUB	- *Professor Liam Murray*
Dental, Belfast Trust	- *Mr Seamus Napier*

Radiation Oncology, Belfast Trust	- *Dr Joe O'Sullivan*
Obstetrics & Gynaecology, Belfast Trust	- *Dr John Price*
Women's Forum Northern Ireland	- *Miss Rosemary Rainey*
Lead Clinician, Western Trust	- *Dr Michael Reilly*

Updated July 2015

APPENDIX D – Extract from GMC Confidentiality guidance: Research and other secondary uses

40. Research, epidemiology, public health surveillance, health service planning and education and training are among the important secondary uses made of patient information. Each of these uses can serve important public interests.

41. For many secondary uses, it will be sufficient and practicable to disclose only anonymised or coded information. When identifiable information is needed, or it is not practicable to remove identifiable information, it will often be perfectly practicable to get patients' express consent.

42. You may disclose identifiable information without consent if it is required by law, if it is approved under section 251 of the *NHS Act 2006*, or if it can be justified in the public interest and it is either:

(a) necessary to use identifiable information, or

(b) not practicable to anonymise or code the information and, in either case, not practicable to seek consent (or efforts to seek consent have been unsuccessful).

43. In considering whether it is practicable to seek consent you should take account of:

(a) the age of records and the likely traceability of patients

(b) the number of records, and

(c) the possibility of introducing bias because of a low response rate or because particular groups of patients refuse, or do not respond to, requests to use their information.

44. When considering whether the public interest in disclosures for secondary uses outweighs patients' and the public interest in keeping the information confidential, you must consider:

(a) the nature of the information to be disclosed

(b) what use will be made of the information

(c) how many people will have access to the information

(d) the confidentiality and security arrangements in place to protect the information from further disclosure

(e) the advice of a Caldicott Guardian or similar expert adviser, who is not directly connected with the use for which disclosure is being considered, and

(f) the potential for distress or harm to patients.

45. When considering applications for support under section 251 of the *NHS Act 2006* in England and Wales, the National Information Governance Board considers:

(a) the feasibility of doing the research or other activity with patients' consent or by using anonymised or coded information, and

(b) whether the use of identifiable information would benefit patients or the public sufficiently to outweigh patients' right to privacy.

46. The Privacy Advisory Committee in Northern Ireland can advise on some of the same considerations; but it has no statutory powers and so cannot give lawful authority to disclosures of identifiable information without consent. In the event of a complaint or challenge, its advice on best practice might play an important part in any assessment of the propriety of a disclosure.

47. The Privacy Advisory Committee in Scotland performs a different role, and doctors there should seek the advice of Caldicott Guardians, defence organisations or professional bodies if they are unsure about whether disclosures of identifiable information for secondary uses can be justified in the public interest.

48. It might not be practicable for the healthcare team, or those who usually support them, to anonymise or code information or to seek patients' express consent:

(a) for the disclosure of identifiable information for important secondary uses, or

(b) so that suitable patients can be recruited to clinical trials or other approved research projects.

49. If that is the case:

(a) identifiable information may be sent to a 'safe haven', where they exist and have the capabilities and are otherwise suitable to process the information (including anonymising or coding it) and to manage the disclosure of information for secondary uses or, if that is not practicable.

(b) the task of anonymising or coding the information or seeking patients' consent to disclosure can be delegated to someone incorporated into the healthcare team on a temporary basis and bound by legal and contractual obligations of confidentiality.

50. You should only disclose identifiable information for research if that research is approved by a Research Ethics Committee. You should alert Research Ethics Committees to disclosures of identifiable information without consent when applying for approval for research projects.

Came into action 12/10/09
Last accessed 12/02/14 http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_40_50_research_and_secondary_issues.asp

APPENDIX E – Data Protection Act 1998 (Extract)

This Act requires the registration of data relating to individuals and held on computer. For all such data it is essential to abide by eight principles which govern the care and use made of the data.

DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in a manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, whenever necessary, kept up-to-date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data Protection Act 1998 (Continued)

SCHEDULE 2 CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1 The data subject has given his consent to the processing.

2 The processing is necessary—
   a) for the performance of a contract to which the data subject is a party, or
   b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 **The processing is necessary—**
   a) for the administration of justice,
   b) for the exercise of any functions conferred on any person by or under any enactment,
   c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
   d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Data Protection Act 1998 (Continued)

Section 4(3).

SCHEDULE 3 CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1 The data subject has given his explicit consent to the processing of the personal data.

2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order—

a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3 The processing is necessary—

a) in order to protect the vital interests of the data subject or another person, in a case where—

i) consent cannot be given by or on behalf of the data subject, or

ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing—

a) is carried out in the course of its legitimate activities by any body or association which—

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6 The processing—

a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
b) is necessary for the purpose of obtaining legal advice, or
c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7 (1) The processing is necessary—

a) for the administration of justice,
b) for the exercise of any functions conferred on any person by or under an enactment, or
c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order—

a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8 **(1) The processing is necessary for medical purposes and is undertaken by—**

a) a health professional, or
b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9 (1) The processing—

a) is of sensitive personal data consisting of information as to racial or ethnic origin,
b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

APPENDIX F – N. Ireland Cancer Registry Confidentiality Undertaking for all Registry Staff

I understand that, in the course of my work, I may come into contact with, or have access to, confidential information relating to individual patients, members of staff or hospitals etc. providing services.

I understand that misuse of this information, especially its disclosure to people or agencies that are not authorised to receive it, would constitute a serious breach of confidentiality. Any breach of confidence will lead to disciplinary action, which may involve dismissal. I also understand that the use and security of personal information is subject to the provisions of the Data Protection Act 1998 and that unauthorised disclosure of personal information is an offence under the Act.

I confirm that I have been given a copy of *"Security Confidentiality and Issue of Data from the N. Ireland Cancer Registry".* This incorporates information, which deals with the handling of confidential information concerned with rules and procedures governing access to cancer registry data. I have read and understood the requirements of the document.

I confirm I have attended training in 'ICT Security and Confidentiality Issues'.

Signed .....

Name in block capitals .....

Job Title .....

Date .....

Witnessed .....

Project Title .....

Project End Date .....

NB: Please return this document, when signed, to the Office Manager

APPENDIX G – Forms relating to release of data from N. Ireland Cancer Registry

Form I - Request for Release of Data from N. Ireland Cancer Registry

Form II - Request for Release of Patient Identifiable Cancer Registry Data

Form IIIa - N. Ireland Cancer Registry Clinician's Permission to Release Data

Form IIIb - N. Ireland Cancer Registry MDT Chair Permission to Release Data
Form IV - Request for Release of Potentially Identifiable Cancer Registry Data

Form V - Confidentiality of Cancer Registry Data Genetic Counselling

Form I - Request for Release of Data from N. Ireland Cancer Registry

N. Ireland Cancer Registry
Centre for Public Health, Mulhouse Building,
Grosvenor Road, Belfast BT12 6DP
Tel: 028 9063 2573 Fax: 028 9024 8017 Email: nicr@qub.ac.uk

DETAILS OF APPLICANT

<table>
<tr><td>Name:</td><td>Title:</td></tr>
<tr><td rowspan="3">Position:

Telephone No:

Fax:

Email:</td><td>Address:</td></tr>
<tr><td>Does the study require
- details of named patients? YES/NO
If yes, Form II will require completion
Form III may also require completion</td></tr>
<tr><td>- Potentially identifiable data? (eg postcodes, cancer type, age group alone) YES/NO
If yes, Form IV will require completion</td></tr>
<tr><td colspan="2">Title of Study:</td></tr>
<tr><td colspan="2">Aims and Purpose of Study:</td></tr>
<tr><td colspan="2">Proposed Methodology [a]:</td></tr>
<tr><td colspan="2">Details of Information Required[a]:</td></tr>
<tr><td colspan="2">Is there a deadline for receipt of information
If YES, please give reason and date.
[a] Append on extra sheet if necessary</td></tr>
</table>

DECLARATION BY APPLICANT

I confirm that data given to me will be used for the purpose for which they are supplied. **I will give the N. Ireland Cancer Registry prior notice of any intended publication based on the data supplied and will acknowledge the NICR as the source of the data and the Public Health Agency for funding the Registry*.** I understand that unless the NICR has participated in the research, any interpretations will be acknowledged to be the author's sole responsibility.

SIGNATURE OF APPLICANT: _____ DATE: _____

* exact wording to be quoted in publication is "The N. Ireland Cancer Registry is funded by the Public Health Agency (PHA)"

Form II - Request for Release of Patient Identifiable Cancer Registry Data

(to be completed in conjunction with Form 1)

N. Ireland Cancer Registry
Centre for Public Health, Mulhouse Building,
Grosvenor Road, Belfast BT12 6DP
Tel: 028 9063 2573 Fax: 028 9024 8017 Email: nicr@qub.ac.uk

1. **Name and Title of Applicant:**
(Please Use BLOCK CAPITALS)

2. **Title of Study**

3. **Are you currently the patient(s) consultant or General Practitioner?** **YES/NO**
(if yes, proceed to 7. Declaration)

4. **Have you (or have you ever had) clinical responsibility for the patient(s)?** **YES/NO**
If 'No' do you require a list of consultants from the N.I.C.R. who
Were responsible for the patients in your study? **YES/NO**
(Please note that we cannot release personal data for patients you are not, or never have been, responsible for unless we receive written permission from the consultants concerned.)

5. **Is Ethical Committee approval required?** **YES/NO**
If 'Yes' please attach necessary confirmation of Ethical Committee's approval for study.

6. Has the patient's consent been achieved? **YES/NO**

7. Declaration

I understand that, in accordance with the Data Protection Act 1998, patient identifiable data is only released providing:

a) The data is only used for the purpose for which they were supplied.
b) The data is not passed on to any other persons or released into the public domain.
c) The data is kept secure at all times.
d) Any results of my work, which are disclosed, shall not be able to identify an individual.
e) The data will not be kept longer that is necessary for the stated purpose and then shall be destroyed by shredding or burning by _____(date)
f) If I become aware of any loss or misuse of the data supplied to me I will inform the Director of the NICR immediately.
g) If I am succeeded in my post with the research project my successor will require to complete a fresh declaration of confidentiality before receiving any further data.
h) I confirm that data given to me will be used for the purpose for which they are supplied. I will give the NICR prior notice of any intended publication based on the data supplied and will acknowledge the NICR as the source of the data and the Public Health Agency which funds the Registry. I understand that unless the NICR has participated in the research, any interpretations will be acknowledged to be the author's sole responsibility.

Signed: _____ Date: _____

IF THE ABOVE SIGNED IS NOT MEDICALLY QUALIFIED PLEASE OBTAIN FURTHER SIGNATURE FROM A MEDICALLY QUALIFIED COLLEAGUE INVOLVED IN THE STUDY/WORK.

DECLARATION BY MEDICALLY QUALIFIED PERSON (If different from person named above)

In accordance with BMA guidelines for release of patient details I undertake to take responsibility for the confidentiality of any data supplied to my colleague involved in the study/work.

Name: (Please Print) _____ Signed: _____ Date: _____

Position: _____ Date of Medical Qualification: _____ GMC Number: _____

Form IIIa - N. Ireland Cancer Registry Clinician's Permission to Release Data

N. Ireland Cancer Registry
Centre for Public Health, Mulhouse Building,
Grosvenor Road, Belfast BT12 6DP
Tel: 028 9063 2573 Fax: 028 9024 8017 Email: nicr@qub.ac.uk

Date:

Consultant:

Address:

Dear Consultant

Re: Use of N. Ireland Cancer Registry Data for Research

I (name of researcher) _____, telephone _____,

email _____, address _____

_____

plan to carry out a study on _____

This would involve obtaining patient identifiable data from the N. Ireland Cancer Registry. The patient(s) research relates to were registered whilst under your care, or that of your predecessor(s). I enclose a copy of the formal request made to the N. Ireland Cancer Registry to release the data. However, before complying, the Registry requires written agreement from the consultant(s) deemed responsible for the registered case(s).

A list of the patients concerned is available from the N. Ireland Cancer Registry. If you require more information on the study outlined above, please do not hesitate to get in contact with me. I would be most grateful if you would complete the section below and return the entire letter to me. I will then give this to the N. Ireland Cancer Registry. This will authorise the release of the data to me, the applicant.

Yours sincerely

(Name of Researcher)

.....

Clinician's Permission:

I consent to the release of data to the applicant for the above named study:

Name: (Please print) _____ Location of Work: _____

Signed: _____ Telephone No: _____

Date: _____ Email: _____

GMC Number: _____

Form IIIb - N. Ireland Cancer Registry Multidisciplinary Team Chair's Permission to Release Data

N. Ireland Cancer Registry
Centre for Public Health, Mulhouse Building,
Grosvenor Road, Belfast BT12 6DP
Tel: 028 9063 2573 Fax: 028 9024 8017 Email: nicr@qub.ac.uk

Date:

Consultant:

Address:

Dear Consultant

Re: Use of N. Ireland Cancer Registry Data for Research

I (name of researcher) _____, telephone _____,

email _____, address _____

_____

plan to carry out a study on _____

This would involve obtaining patient identifiable data from the N. Ireland Cancer Registry. The patient(s) research relates to were registered whilst under your or your colleagues care, or that of your predecessor(s). I enclose a copy of the formal request made to the N. Ireland Cancer Registry to release the data. However, before complying, the Registry requires written agreement from the consultant(s) deemed responsible for the registered case(s).

A list of the patients concerned is available from the N. Ireland Cancer Registry. If you require more information on the study outlined above, please do not hesitate to get in contact with me. I would be most grateful if you would complete the section below and return the entire letter to me. I will then give this to the N. Ireland Cancer Registry. This will authorise the release of the data to me, the applicant.

Yours sincerely

.....

Multidisciplinary Team (MDT) Clinical Lead

I _____ chair of the

_____ MDT have discussed the above study with

colleagues at the MDT meeting and authorise the release of the data.

Signed: _____ Date: _____

Form IV - Request for Release of Potentially Identifiable Cancer Registry Data

N. Ireland Cancer Registry
Centre for Public Health, Mulhouse Building,
Grosvenor Road, Belfast BT12 6DP
Tel: 028 9063 2573 Fax: 028 9024 8017 Email: nicr@qub.ac.uk

1. **Name and Title of Applicant:**
(Please Use BLOCK CAPITALS)

2. **Title of Study**

3. **Has Patient Consent been achieved** **YES/NO**

Declaration

I understand that, in accordance with the Data Protection Act 1998, potentially identifiable patient data is only released providing:

a) The data is only used for the purpose for which they were supplied.
b) The data is not passed on to any other persons or released into the public domain.
c) The data is kept secure at all times
d) No attempt is made to identify information pertaining to particular individuals or to contact individuals.
e) No attempt is made to link the data to other data sets, unless agreed with the NICR.
f) Any results of my work, which are disclosed, shall not be able to identify or potentially identify an individual.
g) The data will not be kept longer that is necessary for the stated purpose and then shall be destroyed by shredding or burning by _____(date)
h) If I become aware of any loss or misuse of the data supplied to me I will inform the Director of the NICR immediately.
i) If I am succeeded in my post with the research project my successor will require to complete a fresh declaration of confidentiality before receiving any further data.
j) I confirm that data given to me will be used for the purpose for which they are supplied. **I will give the NICR prior notice of any intended publication based on the data supplied and will acknowledge the NICR as the source of the data and the Public Health Agency which funds the Registry*.** I understand that unless the NICR has participated in the research, any interpretations will be acknowledged to be the author's sole responsibility.

Signed: _____ Date: _____

* exact wording to be quoted in publication is "The N. Ireland Cancer Registry is funded by the Public Health Agency (PHA)"

Form V - Confidentiality of Cancer Registry Data Genetic Counselling

The policy of the United Kingdom and Ireland Association of Cancer Registries (UKIACR) concerning the release of data for the purposes of genetic counselling requires that a named registered medical practitioner shall be responsible for the confidentiality, use and security of data (see below).

Policy

(i) Requests for cancer registry information from registered medical practitioners working in genetic counselling clinics concerning living family members, related to a proband undergoing counselling should be accompanied by a signed consent form obtained from each family member (or their legal guardian) about whom information is requested. The consent form should permit the release to the named registered medical practitioner of information relating to cancer from medical and hospital records. The consultant and, where possible, the general practitioner responsible for the family member should be informed about the data release.

Information regarding living cancer patients should not be released without their signed consent.

(ii) Information regarding patients known to have died can be released to a registered medical practitioner for counselling purposes, upon request, without consent.

(iii) Registered medical practitioners receiving cancer registry information must undertake to maintain the confidentiality of the data, keep it securely and release it only for counselling purposes. The duty of confidentiality relating to medical information extends beyond death and the above requirements must be adhered to for information relating to both living and deceased patients.

(iv) The information released for counselling purposes should consist of the minimum necessary to achieve the objectives required. In normal circumstances this would comprise; name, address, date of birth, date of diagnosis, cancer site and histology, name and hospital of managing consultant and (for living patients) name and address of GP.

Name of Medical Practitioner responsible:

.....
.

I declare that I understand and agree to act in accordance with the UKIACR policy.

Signature ..... Date .....

Name of recipient if not the medical practitioner whose name is given above.

.....

APPENDIX H – Example Data Requests

Listed below are the four main categories of requests the NICR expects to receive.

Category 1. Aggregated Data

Data of this type are numbers of patients broken down by gender, age, site or geographical location. Requests of this type would normally be freely available to all enquirers, subject to resource implications. Examples of this type of request are:

(a) The number of kidney cancer deaths over the past five years at different age periods, by gender.

(b) The number of lung cancers registered in each District Council Area at five year age periods, by gender.

Note: For some rarer cancers the breakdown of numbers may be limited to protect the confidentiality of the information.

In some cases, aggregated data may be regarded as potentially identifiable. If potentially identifiable, data will not be released until the Director of the NICR is satisfied that the person to whom the data will be sent is working in an established organisation and takes responsibility for the information supplied.

Category 2. Data Traceable to an Individual Patient

(see para 2.2 *"Confidentiality Guidelines for Staff Working in the N. Ireland Cancer Registry"* for definition of data which may identify a person).

Data of this type will not be released until the Director of the NICR is satisfied that the clinician responsible for the patient has consented to the release of the information and the person to whom the data will be sent is either medically qualified, or is working with a co-researcher who is medically qualified, and takes clinical responsibility for the information supplied. Where necessary the appropriate ethical approval must also be obtained. Examples of this type of request:

(a) List of patients (names or hospital numbers) with bone cancer over the past three years.

(b) Number of patients registered with testicular cancer in a rural area over the past five years. (Problem arises in that the small numbers may identify individuals).

Category 3. Data on a Clinician's Own Patients

A clinician's own data sent to the Registry, or any data the clinician now has responsibility for (e.g. that of their predecessor), are freely available to that clinician. Requests should be presented to the Director in writing. Examples of this type of request:

(a) List of patients with bone cancer I have treated over the last three years.
(b) Has patient *"Mr Smith"*, whom I treated two years ago, died?

Category 4. Data Traceable to an Individual Clinician or Caring Institution

Data of this type will not be released until the Director is satisfied that the clinician, or all clinicians working in an institution, have given their consent to release the information about them. Examples of this type of request:

(a) List of all patients treated by the consultants responsible for urology cancers in the past year.

(b) Survival of patients treated at *Institution X* in 1990. (This information would normally only be available for a clinical audit situation where rules of confidentiality apply).

HSCNI Secure Email Service

User Guide

Produced by the BSO ITS Security Team
Version 1.0

Version Control

V0.1	Initial draft	16/03/2011
V0.2	Updated images to reflect HSCNI styling and password recovery	21/11/2011
V1.0	Updated to reflect live service for all HSC outbound traffic	03/09/2012

Contributors

Michael Harnett

Table of Contents

Introduction

This document provides guidance on how HSC staff can encrypt email when it is being sent to a recipient outside the HSCNI and GP networks.

Encryption must be applied to any content that is deemed sensitive or contains patient information.

Examples of sensitive and personal information include but are not limited to:-

- copies or extracts of data from clinical systems;
- commercially sensitive information;
- contracts under consideration;
- budgets;
- staff reports;
- appointments – actual or potential not yet announced;
- disciplinary or criminal investigations.

Personal information is further defined by the Data Protection Act (1998).

Pre-requisites

1. The recipient's organisation must allow encrypted attachments through their quarantine procedures. Therefore encrypted email to the Police Service NI and the NI Court's Service cannot be sent using this method.

2. Procedures should be agreed between the sender and recipient on how the service should be used i.e.
    - All sensitive/personal data to be in an attachment rather than the body of the email.
    - Acknowledgement of receipt.

Caveats

1. An encrypted email exchange must be initiated from within the HSC.

2. GPs cannot use this service as their email service does not the HSC email gateway.

3. It will not encrypt email between HSC organisations including the GPs.

4. The password applied to an encrypted email will always remain the one the recipient had set at the time the email was sent. Therefore if a recipient resets their HSC Encrypted Email Service password they must use their old password to open old encrypted emails. If the recipient forgets their password they will not be able to access old encrypted emails.

5. Due to a security restrictions within Adobe Reader default settings, executable (*.exe) and compressed (*.zip) files cannot be transferred using this service.

6. The size of attachments are restricted to 10Mb by the HSC organisations.

Notes on Current Configuration

1. The service has the ability to automatically encrypt emails if certain criteria are meet. Examples of these are:
   Specific sender,
   Specific recipient,
   Email or attachment contains Health & Care numbers,
   Email or attachment contains postcodes,
   Email contains a certain phrase or word.

   Please contact Michael Harnett (Michael.harnett@hscni.net) if you want to discuss automatic encryption rules.

A Worked Example

In this example the

Sender email address is Michael.harnett@hscni.net and the

Recipient email address is secteam304@gmail.com

Sections **1**, **14** and **15** below apply to the sender.

Sections **2-4** below are only completed the first time a recipient receives an encrypted email from an hscni.net email address.

Sections **5-9** below show how a recipient opens an encrypted email.

Sections **10-13** below show how a recipient replies with an encrypted email.

Sections **16-17** below shows how a recipient can reset or recover their password.

1. Sending an Encrypted Email

The encryption of all external email is not automatic as the vast majority do not need to have encryption applied and could potentially increase the management overhead for the Email teams of the recipient organisations.

To manually encrypt an email, the sender creates a new email and includes **[ENCRYPT]** in the Subject line (see Figure 1). The square brackets **[ ]** are required.

Figure 1

2. Recipient Registering with the HSCNI Encrypted Email Service

The first time the recipient is sent an encrypted email from an HSC email address using this service, the recipient must register their email address with the HSCNI Email Encryption Server.

To do this, the recipient will receive an email with contents similar to Figure 2.

To register with the service, click on the **here** link, circled in red in Figure 2.

If the email program does not support active links, then copy and paste the link circled in orange into your internet browser.

Figure 2

3. Recipient setting their password

This will open the default internet browser, i.e. Internet Explorer, on the recipient's PC and Figure 3 is displayed.

The recipient then completes the **Password** and **Confirm Password** fields.

The complexity of the password required is displayed in the **Password Requirements** box.

NOTE: The ✖ changes to a ✔ when the password meets the password requirement. All three need to change to ✔ before the recipient can proceed.

The recipient must then select 3 questions from the drop down list in the **Password Reset/Recovery** section and enter 3 answers. This will allow the recipient to reset or recover their password if required at a later date without having to contact the BSO Service Desk.

When all fields are completed the recipient can then click on the **Register** button to complete the process.

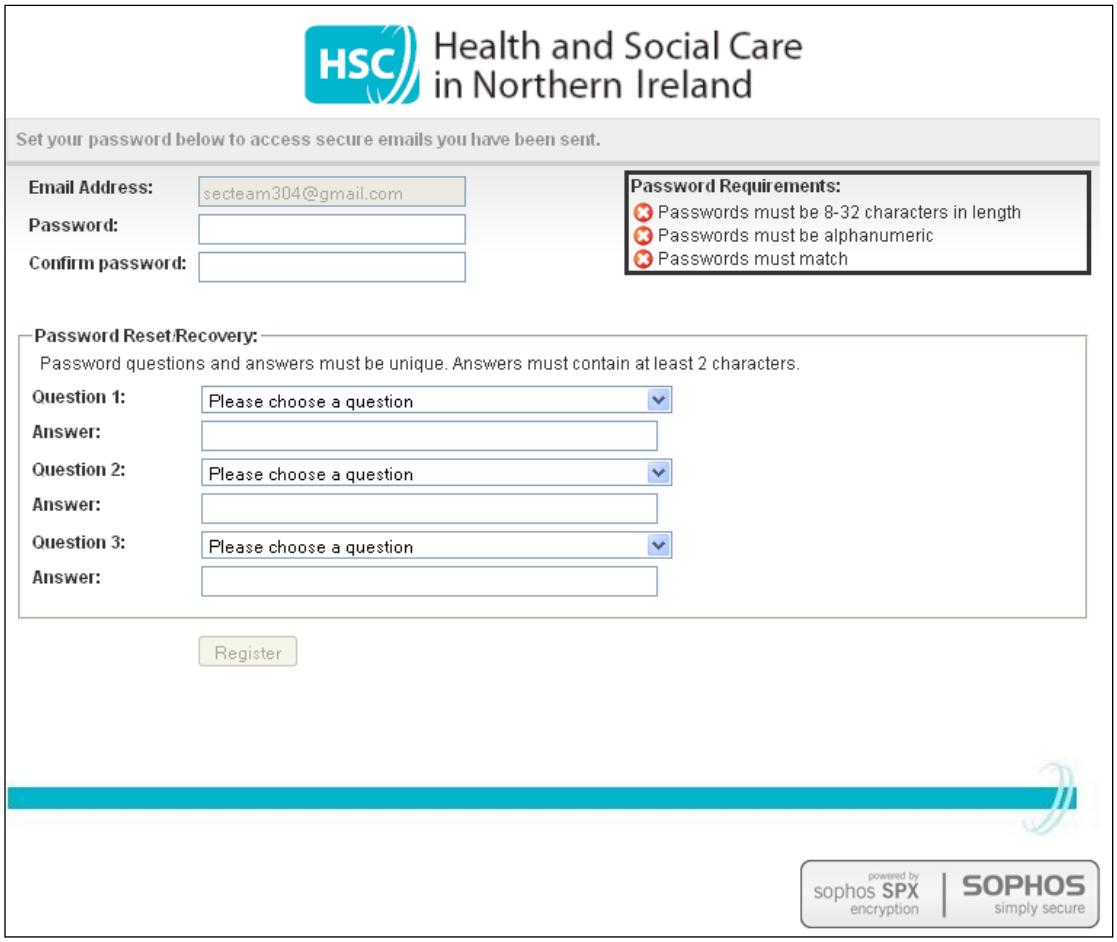

Figure 3

4. Registration confirmation

When the registration has been successfully completed, the recipient will receive a notification as in Figure 4.

This internet browser window can be closed.

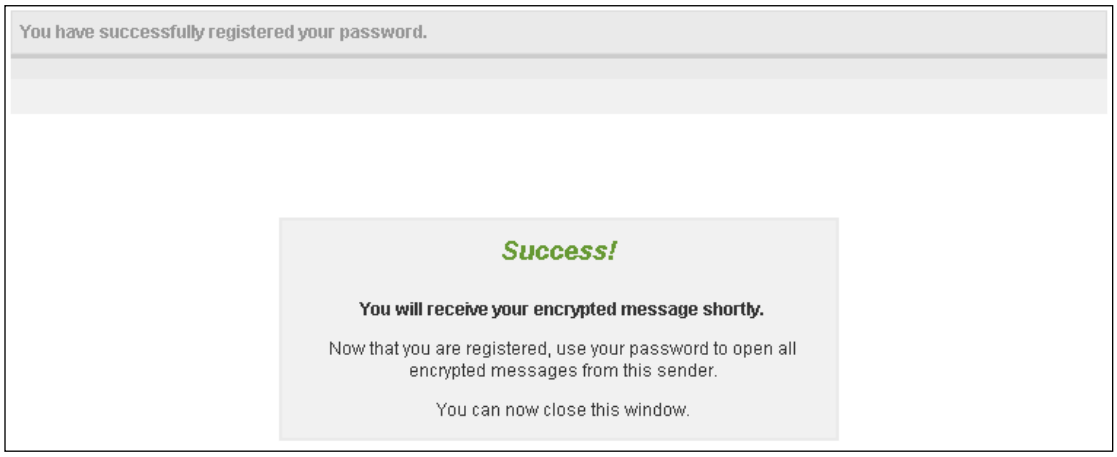

Figure 4

5. Recipient receiving the encrypted email

The recipient will now receive another email which contains the original content from the sender - see Figure 5.

To access that content, the recipient should click on the **PDF logo** at the bottom of the message, circled in red in Figure 5.

Figure 5

6. Recipient receiving the encrypted

The recipient will then see a **File Download** window on their screen – see Figure 6

Click the **Open** or **Save** button to progress.

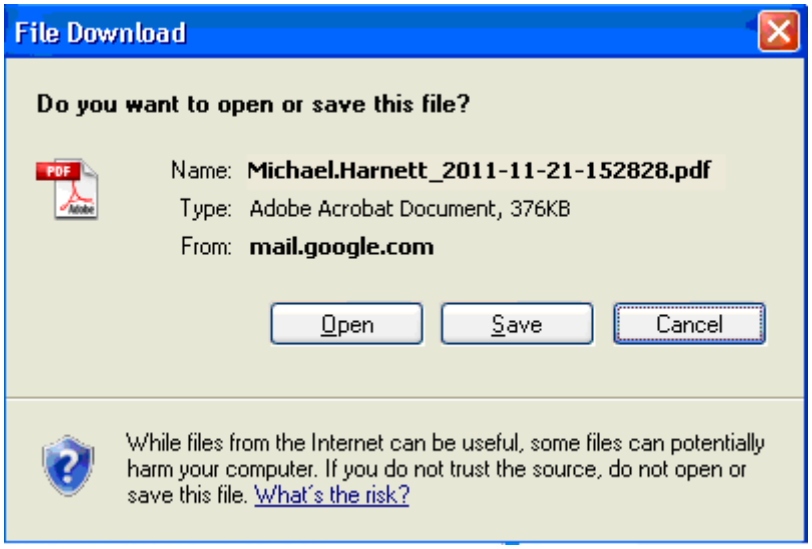

Figure 6

7. Recipient enters their password

The recipient enters the password they registered in Section 3 above, in the **Password** window – see Figure 7.

Then click the **OK** button.

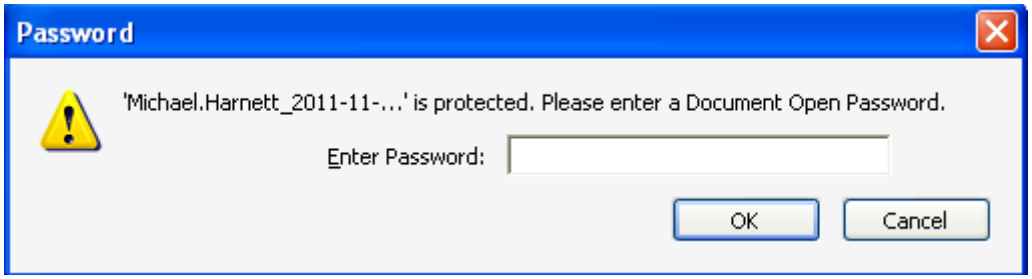

Figure 7

8. Recipient accesses the decrypted email

Attachments may be found at the bottom of the PDF or in a column to the left of the content, depending on the version of Adobe Reader used – see Figure 8.

NOTE: To remove the need to constantly re-enter the password for the PDF, the attachments can be saved to the recipient's file store.

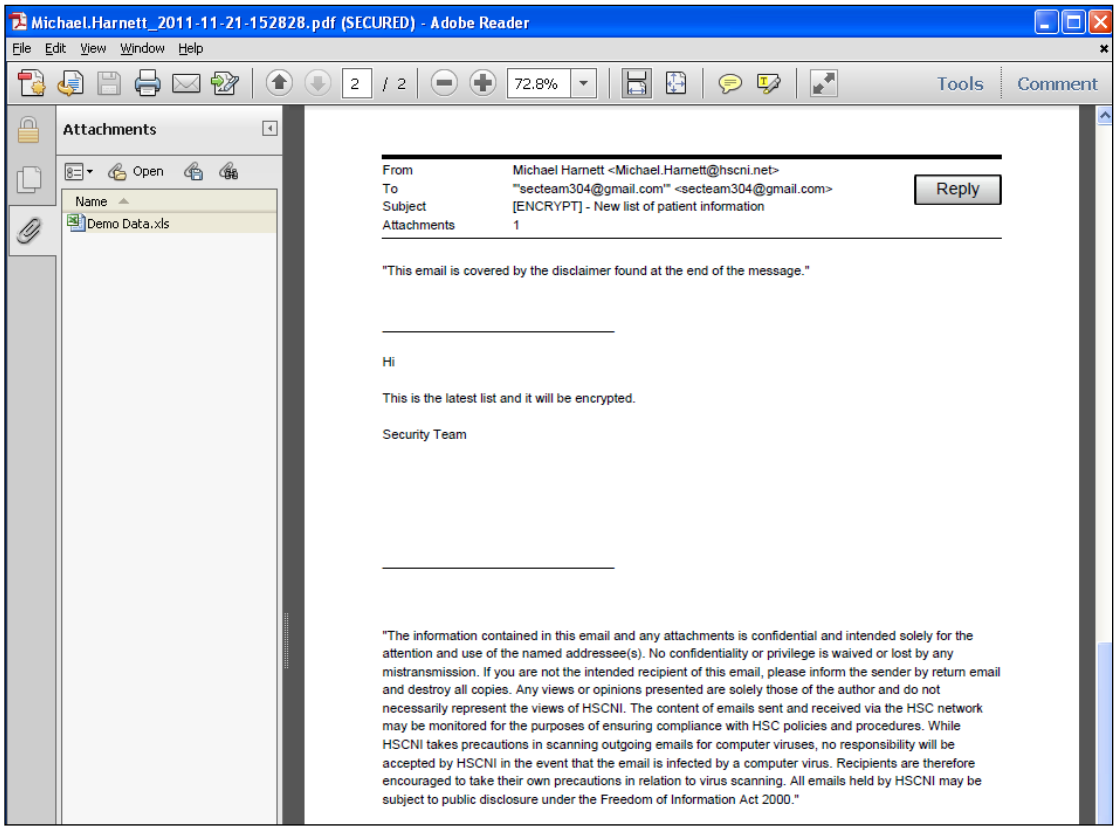

Figure 8

9. Recipient replies with an encrypted email

The recipient clicks on the **Reply** button and Figure 9 may be displayed depending on the security settings within the recipient's organisation.

Click on the **Allow** button to progress.

NOTE: By ticking the **Remember my action for this site** box, this action will not be required for further emails from this service.

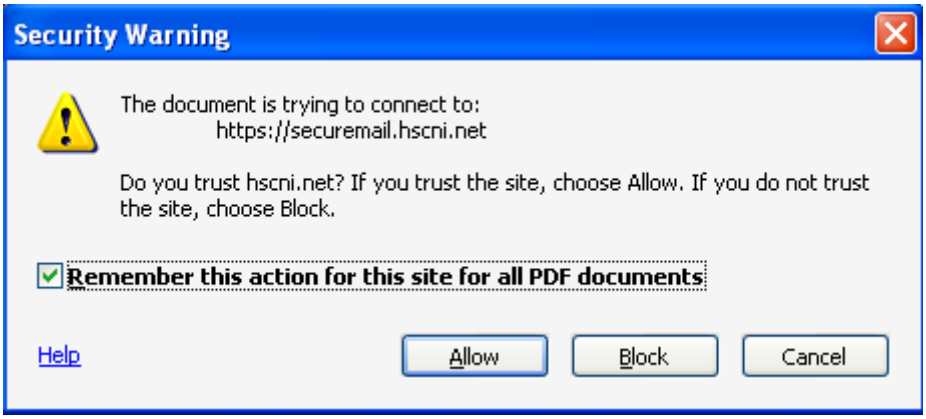

Figure 9

10. Recipient composing reply

Enter the content of the reply as normal – see Figure 10

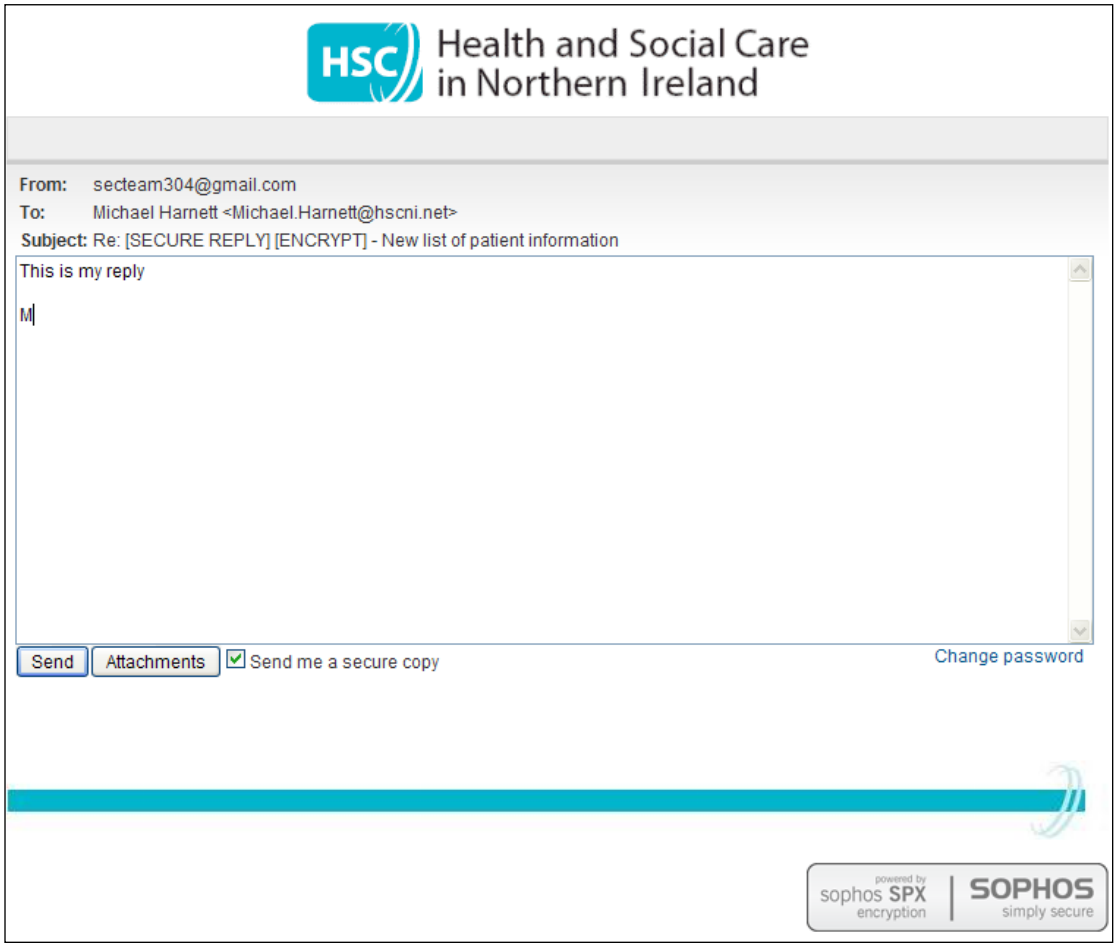

Figure 10

11. Recipient adding attachments

To add an attachment, click on the **Browse** button and navigate to the file to be attached as per the normal operating system browsing method.

Once selected, click the **Upload** button. This will display the uploaded file in the **Attachments** column – see Figure 11.

Repeat this process for all files that need to be attached.

Click the **Done** button to return to email.

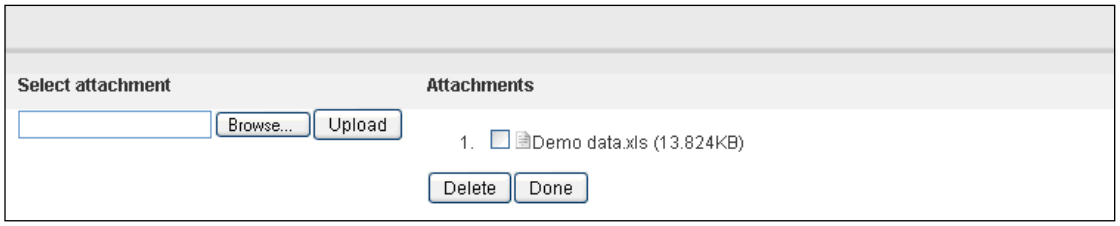

Figure 11

12. Recipient sending the encrypted reply

The attachment added from Section 11 is displayed.

Click on the **Send** button.

Unselect the **Send me a secure copy** if a copy is not required.

NOTE: This service does not save a copy to the **Sent Items** folder, therefore if confirmation that the email was sent is required, this box should be left ticked.

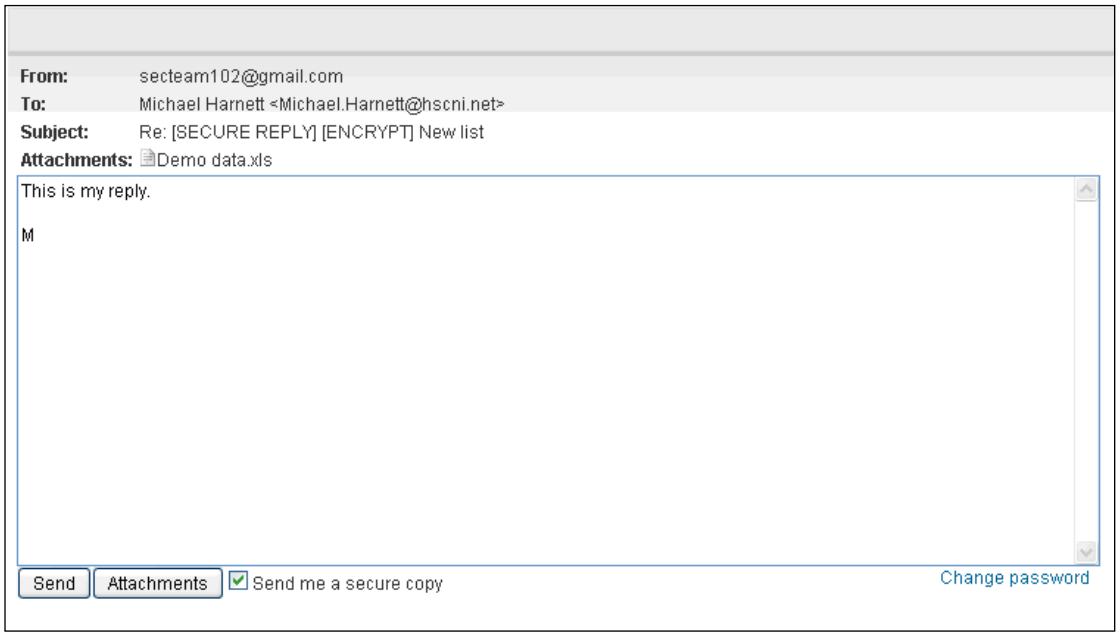

Figure 12

13. Recipient receives sent confirmation

The recipient will receive a confirmation window if the message is sent successfully – see Figure 13.

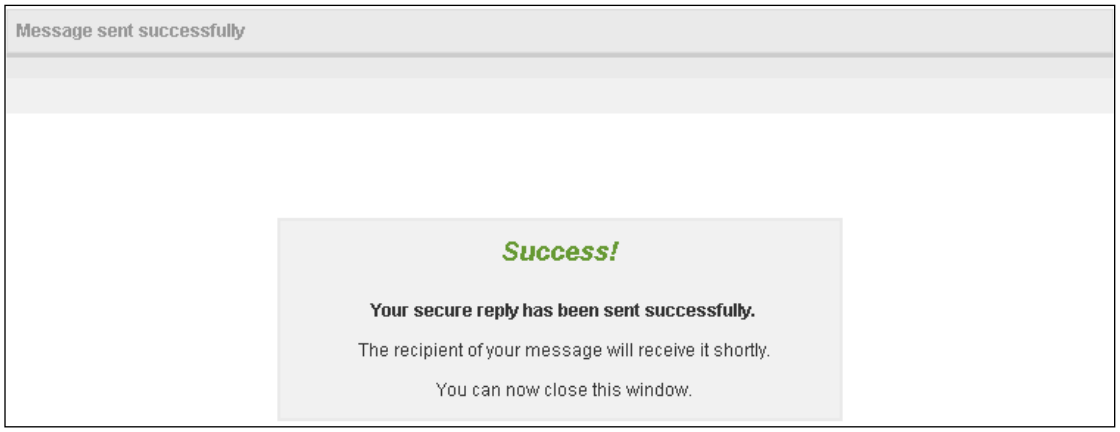

Figure 13

14. Sender receives confirmation the email is encrypted

When the sender's email is encrypted, i.e. includes **[ENCRYPT]** in the subject line, a confirmation is received to say it was successfully encrypted – see Figure 14.

NOTE: This email will not be received until the recipient has registered with the HSC service. Therefore there will be a delay in receiving this confirmation when sending to a recipient for the first time.

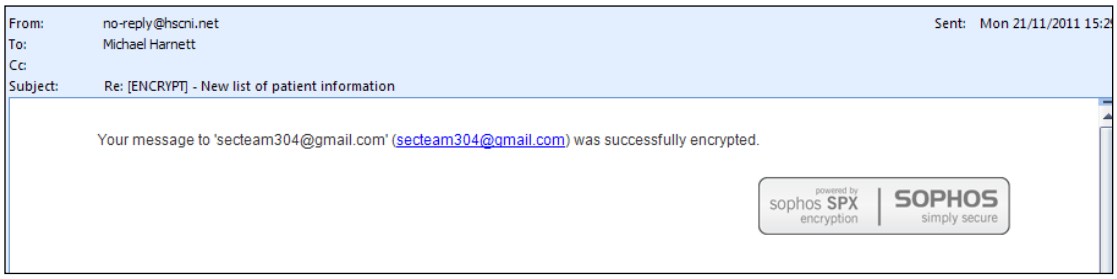

Figure 14

15. Sender receives reply from Recipient

Replies received from the recipient will be decrypted automatically by the HSC Encrypted Email Service and then forwarded into the Sender's mailbox – see Figure 15.

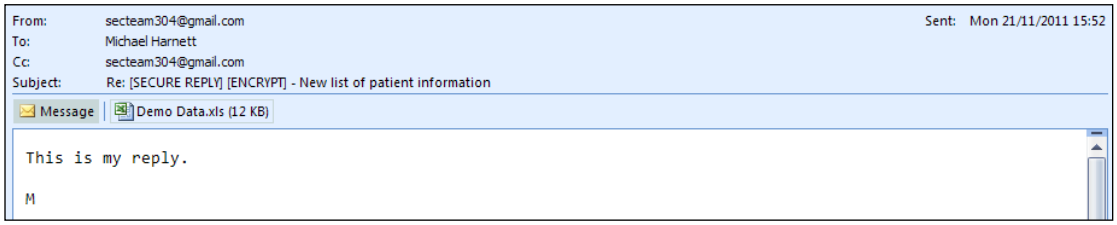

Figure 15

16. Recipient resetting the password

If a recipient believes their password to be compromised they can reset their password using the appropriate link from a previously received encrypted email from the HSCNI Encrypted Email Service.

The links are found in the body of email – see Figure 16

NOTE: The recipient can only use an email sent to them as the links contain references to their email address.

NOTE: All previous encrypted emails will still require the old password to open.

Figure 16

To change the password, click the appropriate link, enter the **Current password**, and then the new password in the **Password** and **Confirm Password** fields – see Figure 17.

Figure 17

Once the password criteria are meet i.e. all have a ✓ against then, click the **Change Password** button to complete the process.

The recipient can also update the **password change/recovery questions** by ticking the box – see Figure 18.

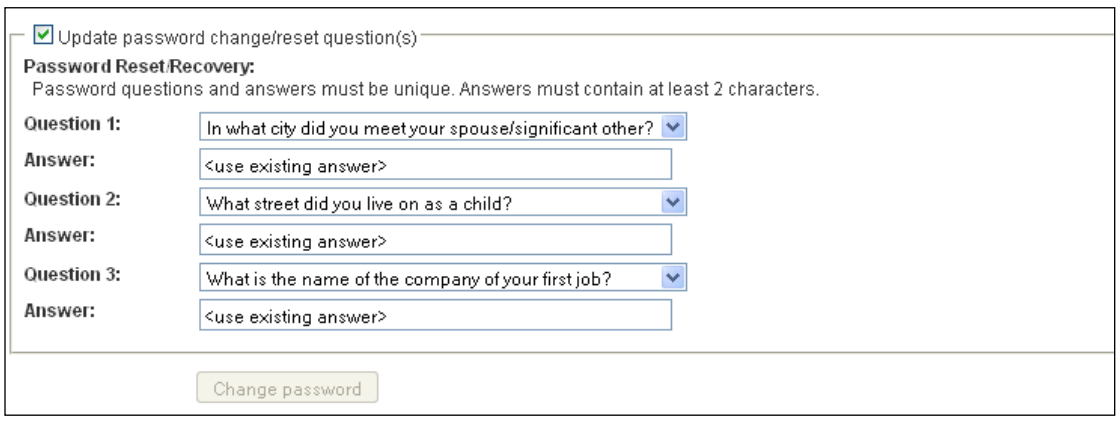

Figure 18

The Change Password button will remain greyed out until all 3 answers are entered.

NOTE: The previous answers can be re-entered.

Notification will be displayed when the password has been successfully changed – see Figure 19.

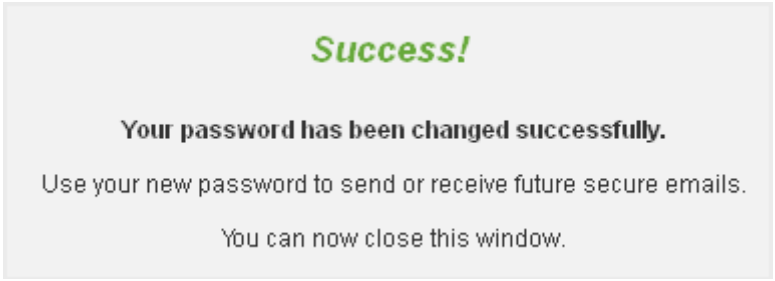

Figure 19

17. Recipient recovering the password

If a recipient forgets their password they can recover it by using the appropriate link from a previously received encrypted email from the HSCNI Encrypted Email Service.

The links are found in the body of email – see Figure 20

NOTE: The recipient can only use an email sent to them as the links contain references to their email address.

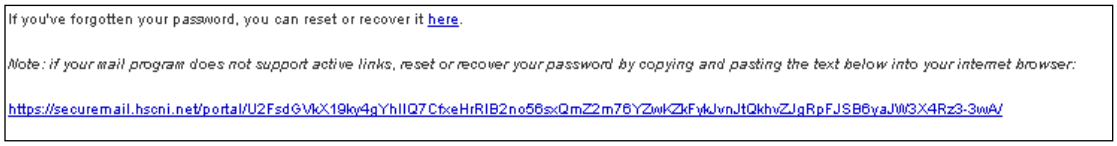

Figure 20

The following window will open in the default internet browser – see Figure 21.

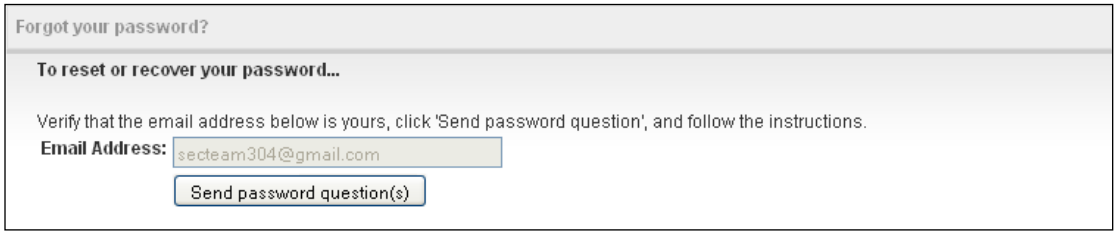

Figure 21

Click on the **Send password Question(s)** button to send them to your email address. On successful completion a notification will be displayed in the internet browser – see Figure 22.

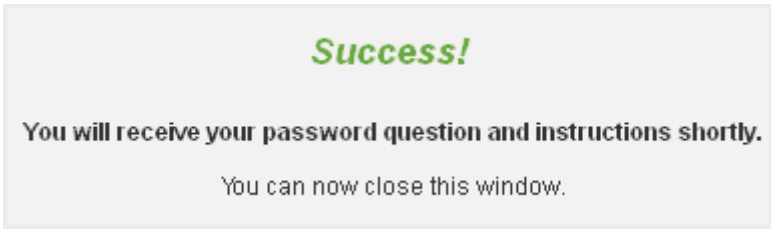

Figure 22

The recipient will receive an email with a link to preset questions – see Figure 23.

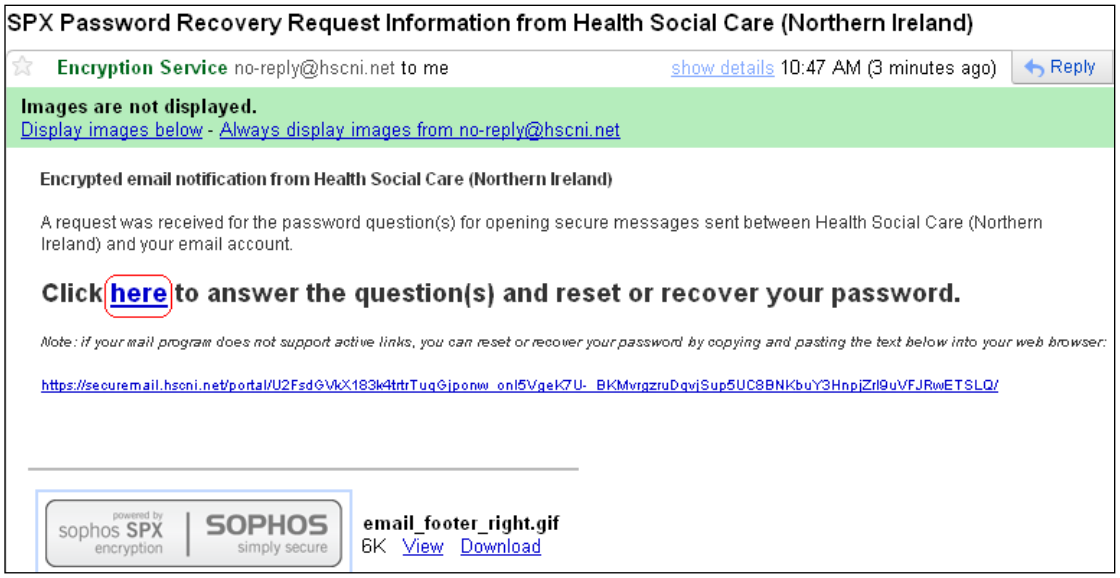

Figure 23

A new internet browser window will open to allow entry of the answers to the preselected questions and the option to recover or reset the password – see Figure 24.

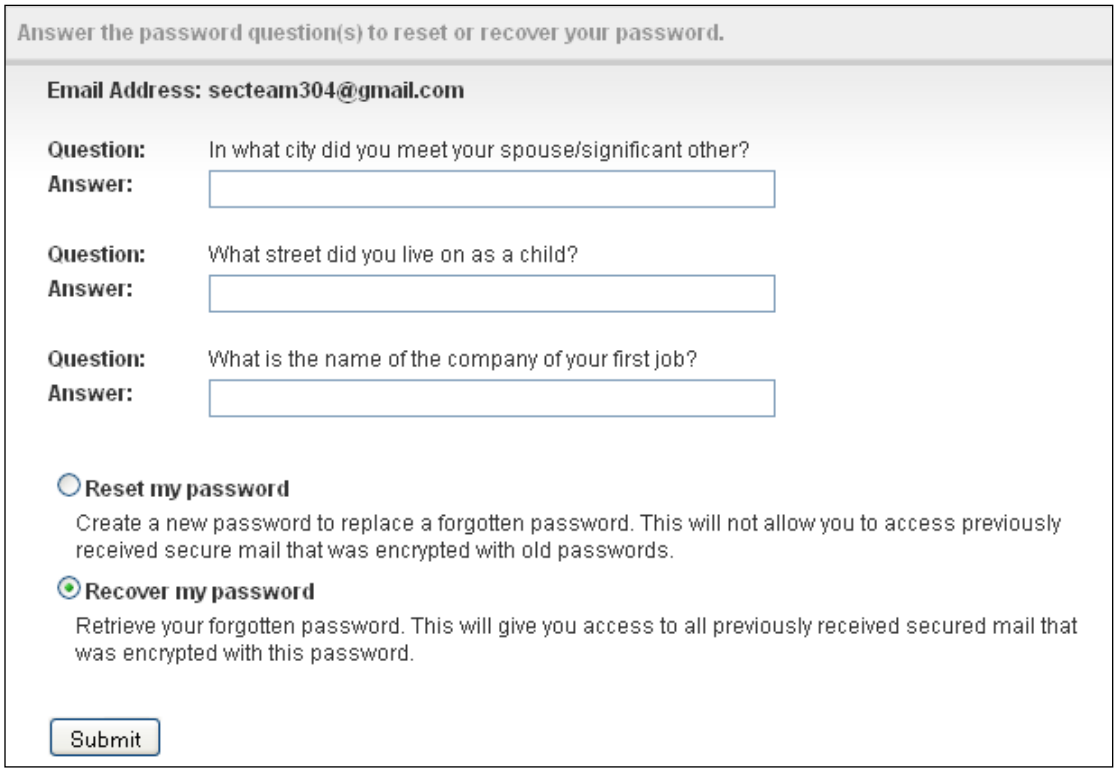

Figure 24

Enter the 3 answers, select **Recover my password** and click the **Submit** button.

NOTE: When an answer is entered incorrectly, the screen will be reset and **Invalid answer** will be displayed in place of **Answer the password question(s) to reset or recover your password**.

The screen will display a temporary one time password (circled in red) that the recipient will need to use to open a new encrypted email that will contain their password – see Figure 25.

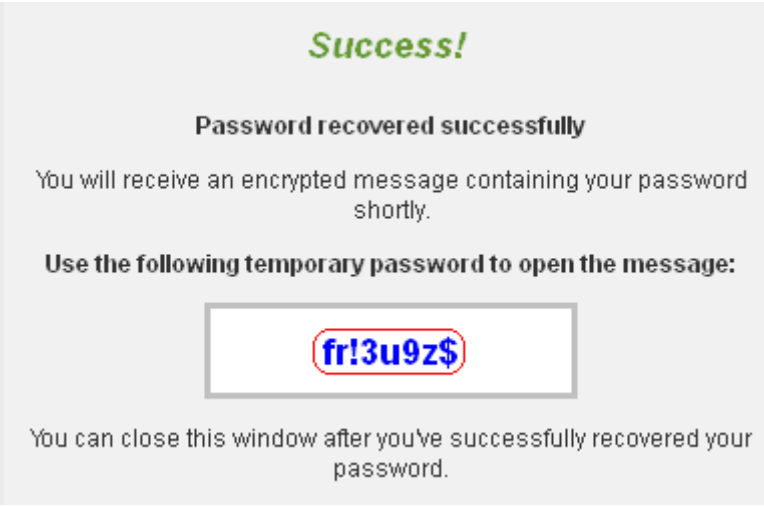

Figure 25

The recipient must now open the email with a subject title - **SPX Password Recovery Request Information from Health Social Care (Northern Ireland)**

Open the attached PDF attachment – see Section 5 for further details if required.

The PDF will contain their password.

NOTE: It is recommended that this message is deleted immediately after the password has been confirmed.

18. Who to contact if there are problems

If you are experiencing issues or have any queries about the HSC Encrypted Email Service you should contact the **BSO ICT Service Desk** (Tel: 028 9054 2400 Email: supportteam@hsci.net).