HSC Secure Email Service

User Guide

Produced by the BSO ITS Security Team
Version 1.9

Version Control

V0.1	Initial draft	16/03/2011
V0.2	Updated images to reflect HSC styling and password recovery	21/11/2011
V1.0	Updated to reflect live service for all HSC outbound traffic	03/09/2012
V1.1	Updated to reflect CJSM and time limits on usage	28/11/2012
V1.2	Update with Recipient password reset, expiration date and Outlook Add-in	02/05/2013
V1.3	Update to BSO-ITS Service Desk contact phone number	24/06/2013
V1.4	Updated to reflect NHS mail to remain over N3	30/07/2013
V1.5	Supported version of pdf reader added	02/08/2013
V1.6	Minor changes to email routing exceptions	06/02/2014
V1.7	Changes to email routing exceptions including RQIA and expiry dates	16/12/2015
V1.8	Added Lisburn & Castlereagh Council * PHE email to service	26/02/2016
V1.9	Changes to RQIA email routing and added exceptions for Office for NI Ombudsman, NFI and Waltham Forest Council.	25/11/2016

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 HSC 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. The Recipient would need to check with their IT team. If the Recipient does not receive an email it may be trapped by their Email Quarantine service.

2. The Recipient requires Adobe Reader V9 or later to open the pdf files that are encrypted. ***To view the attachments, the Recipient may need to toggle the Navigation menu on by pressing F4. Other pdf readers may work but are not supported.***

3. Procedures **should be agreed** between the Sender and Recipient on how the service should be used i.e.

    - Test the process is working as expected before sending the first sensitive/personal data.
    - All sensitive/personal data to be in an attachment rather than the body of the email and t**he attachment extracted from the email on delivery.** This removes the need to retain passwords for old emails
    - Acknowledgement of receipt.

Caveats

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

2. It will not encrypt email between HSC organisations including the GPs and RQIA (hscni.net and n-i.nhs.uk).

3. It will encrypt email between an HSC organisation and the following exceptions to the general rules listed below in Caveat 4

Mail domain	Description
@nissa.gsi.gov.uk	Social Security Agency GSI accounts
@ir-efiles.gov.uk	HM Revenue and Customs
@lisburncastlereagh.gov.uk	Lisburn & Castlereagh City Council
@phe.gov.uk	Public Health England
*hcn.n-i.nhs.uk	H&C Number server monitoring
@walthamforest.gov.uk	Waltham Forest Council
@nfi.gov.uk	National Fraud Initiative

4. The following email domains are not routed through this service and therefore not encrypted by it:

Mail domain	Description
*.hscni.net	HSC email domains
*.n-i.nhs.uk	HSC legacy mail domains and GPs
*.nhs.uk	Mainland NHS organisations
@nhs.net	NHS mail
*.cjsm.net	Criminal Justice Secure Mail
*ni.gov.uk	Northern Ireland Government Departments
*nigov.net	Northern Ireland Government Departments
*.gov.uk	Mainland Government Departments
*.gsi.gov.uk	Government Secure Intranet
*.hmrc.gov.uk	HM revenue and Customs
*.nihe.gov.uk	NI Housing Executive
@ccea.org.uk	Council for the Curriculum, Examinations and Assessment
@hiainquiry.org	Historical Institutional Abuse Inquiry
@sportscouncil-ni.org.uk	Sports Council NI
@ihrdni.org	Inquiry into Hyponatraemia-related Deaths
@nipso.org.uk	Office of the NI Public Services Ombudsman
*.police.uk	All UK Police forces

5. **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.**

6. Certain file types cannot be opened by Adobe Reader when attached to encrypted SPX email messages. These file types include but are not limited to:
   *.exe – executable files
   *.zip – compressed files
   *.bat – batch files
   *.dll – dynamic libraries
   *.class – java class

7. The size of attachments is restricted to 10Mb for all HSC organisations.

Notes on Current Configuration

1. The service has the ability to automatically encrypt emails if certain criteria are met. 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 HSC ICT Security Manager (ictsecuritymanager@hscni.net) at BSO ITS ICT Security if you want to discuss adding 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**, **2**, **3**, **16** and **17** below apply to the Sender.

Sections **4-6** below are only completed the first time a Recipient receives an encrypted email from an hscni.net email address.

Sections **7-11** below show how a Recipient opens an encrypted email.

Sections **12-15** below show how a Recipient replies with an encrypted email.

Sections **18-19** below shows how a Recipient can reset or recover their password.

1. Sending an Encrypted Email using the manual process

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. Sending an Encrypted Email using the Outlook Add-In

This requires your organisation to have deployed the Outlook Add-in for the Secure Email Service. This will appear as a menu option or icon when you create a new email.

By default all new emails will have the encryption turned off and the icon will appear as Figure 2.

When you click on it to apply encryption is changes to highlight its selection as in Figure 3.

Figure 2

Figure 3

If encryption is selected in error, clicking on the Encrypt icon again will turn it off.

Note: This **does not** encrypt email sent to other hscni.net email accounts.

3. Confirmation to the Sender of Encryption

Within a few minutes the Sender will receive confirmation that the email will be encrypted – see Figure 4 as an example.

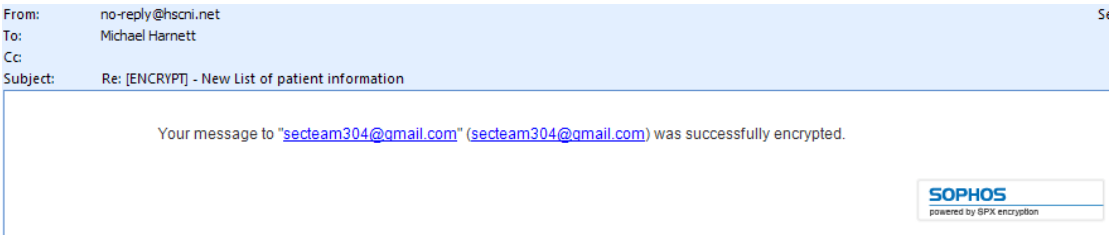

Figure 4

4. Recipient Registering with the HSC Secure 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 HSC Email Encryption Server.

To do this, the Recipient will receive an email with contents similar to Figure 5.

To register with the service, click on the **here** link, circled in red in Figure 5.

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

Figure 5

NOTE: A Registration Reminder email will be issued after 5 days if registration has not taken place.

NOTE: After 10 days the Recipient will not be able to register to receive the email, the email will be deleted and the Sender notified.

NOTE: The Sender is notified when the Recipient has successfully registered.

5. Recipient setting their password

This will open the default internet browser, i.e. Internet Explorer, on the Recipient's PC and Figure 6 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.

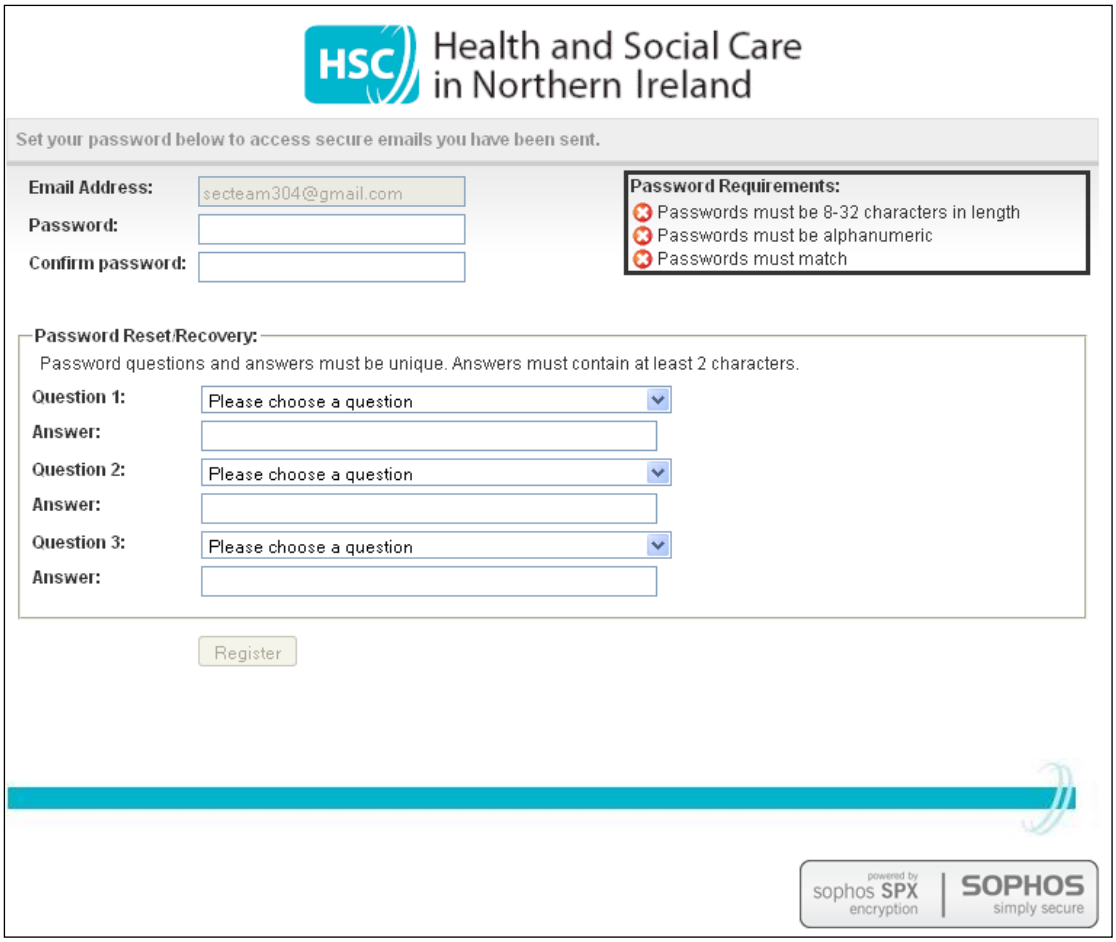

Figure 6

6. Registration confirmation

When the registration has been successfully completed, the Recipient will receive a notification as in Figure 7.

This internet browser window can be closed.

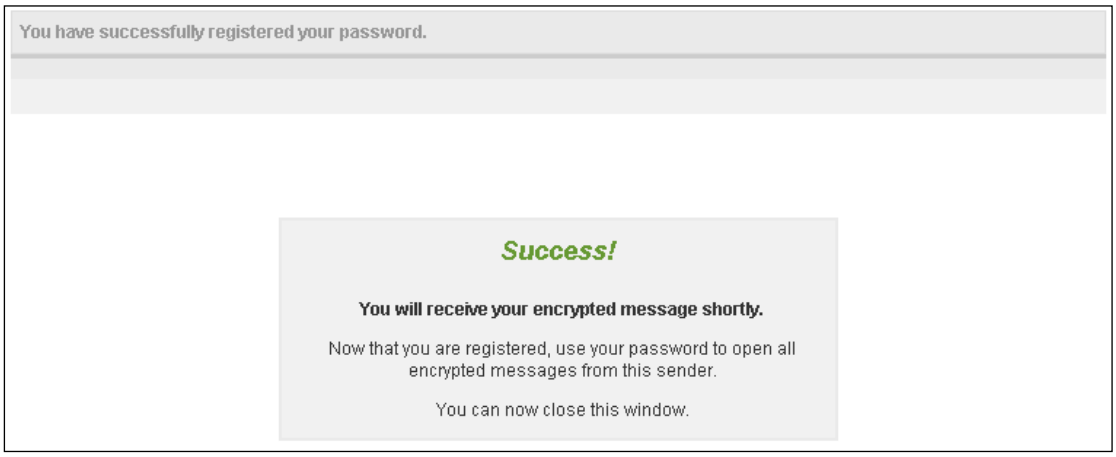

Figure 7

7. Recipient receiving the encrypted email

The Recipient will now receive another email which contains the original content from the Sender - see Figure 8.

To access that content, the Recipient should click on the **PDF logo** at the bottom of the message, circled in red in Figure 8.

Figure 8

8. Recipient receiving the encrypted

The Recipient will then see a **File Download** window on their screen – see Figure 9.

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

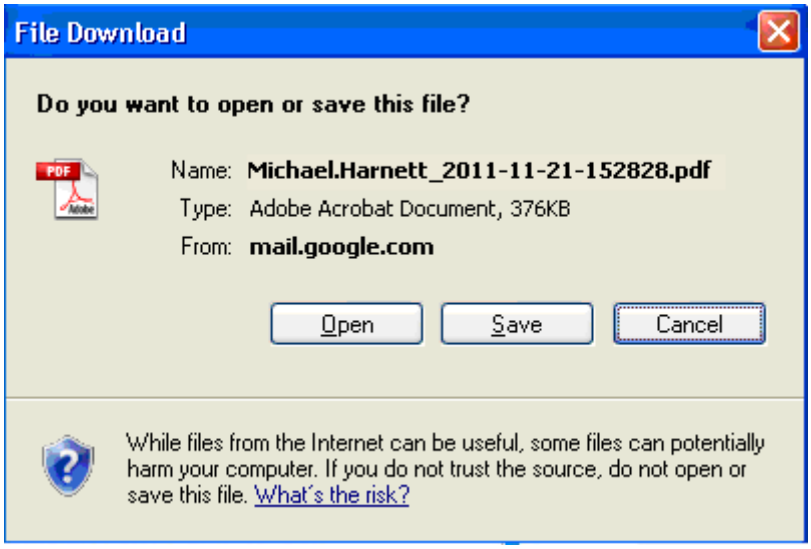

Figure 9

9. Recipient enters their password

The Recipient enters the password they registered in Section 3 above, in the **Password** window – see Figure 10.

Then click the **OK** button.

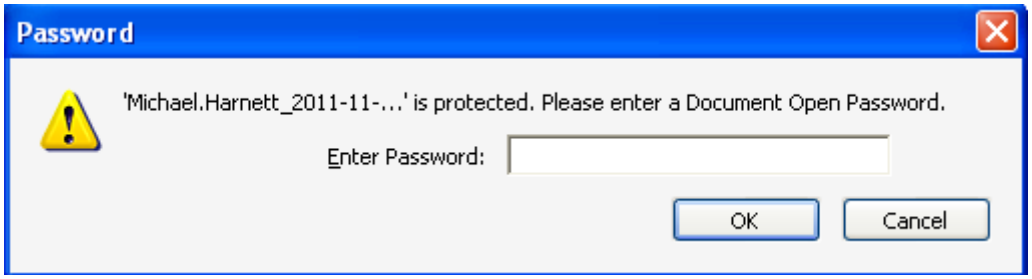

Figure 10

10. 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 11.

TIP: F4 toggles the Navigation pane on the left hand side off and on. If you cannot see the paperclip icon press F4.

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.

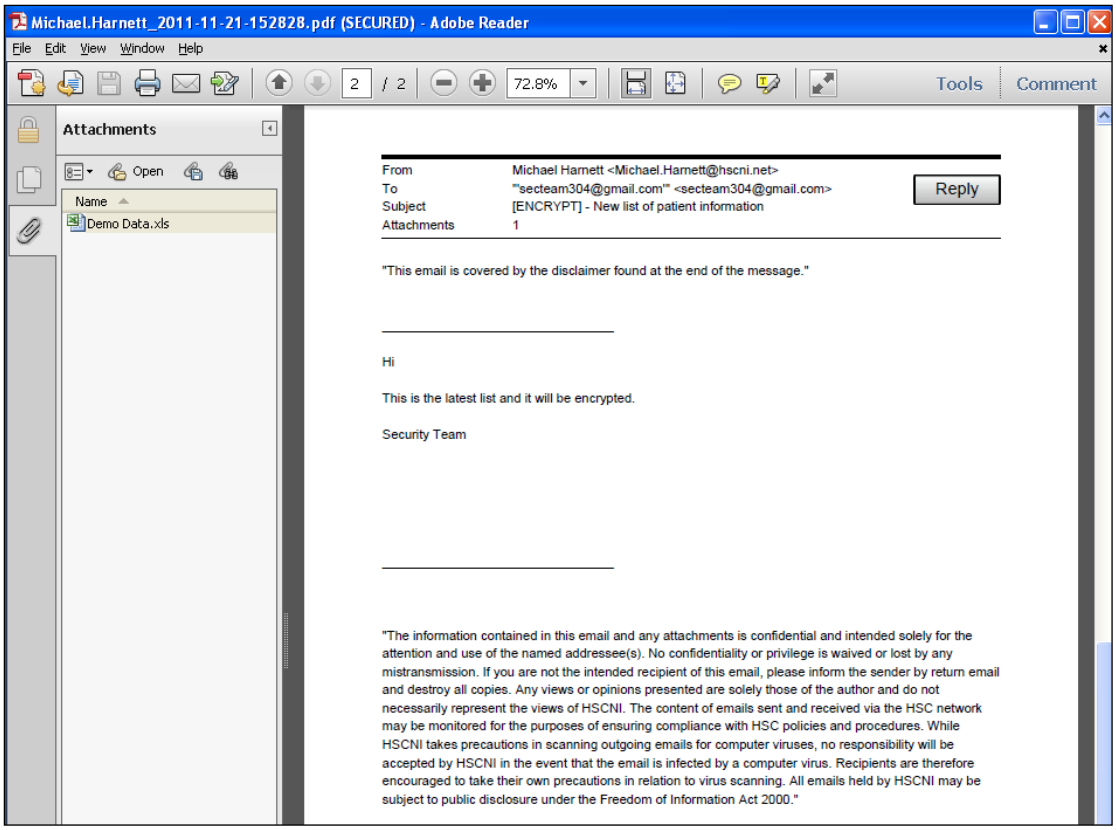

Figure 11

11. Recipient replies with an encrypted email

The Recipient clicks on the **Reply** button and Figure 12 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.

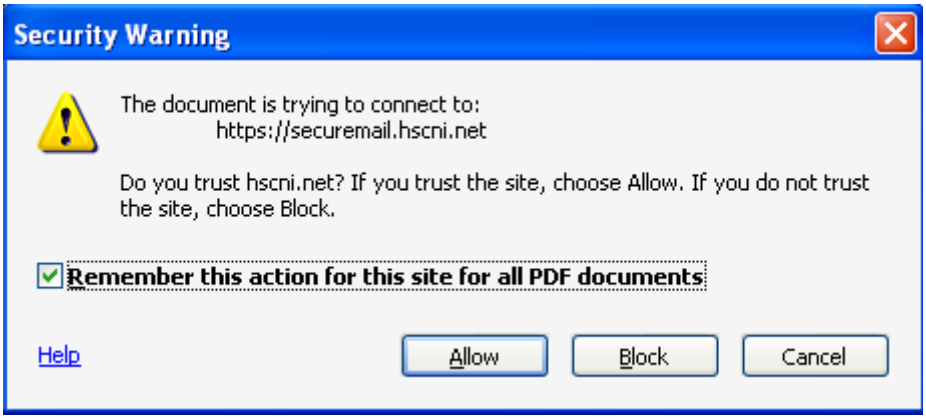

Figure 12

NOTE: The **Reply** functionality to a particular email is 30 days from the date of issue. Please request another secure email from the Sender if it is beyond the 30 days and your response contains sensitive information.

12. Recipient composing reply

Enter the content of the reply as normal – see Figure 13

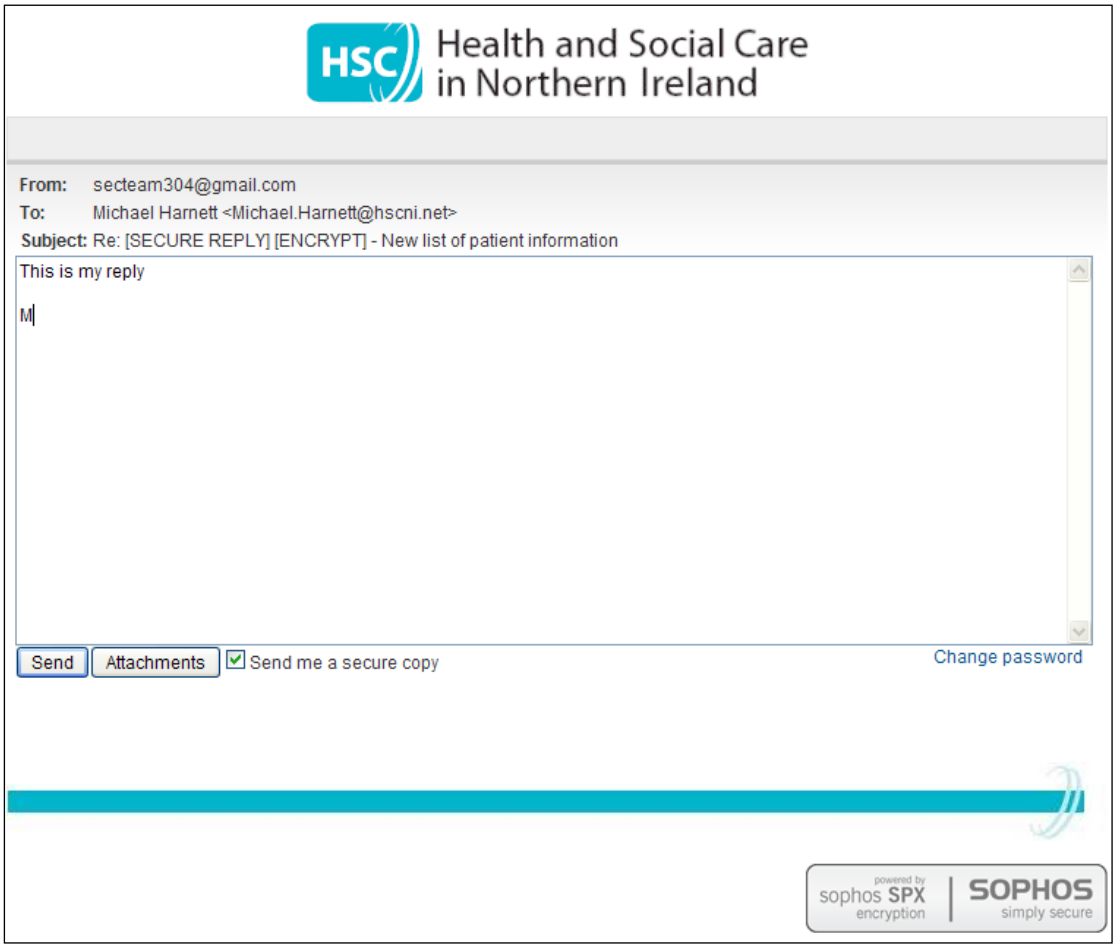

Figure 13

13. 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 14.

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

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

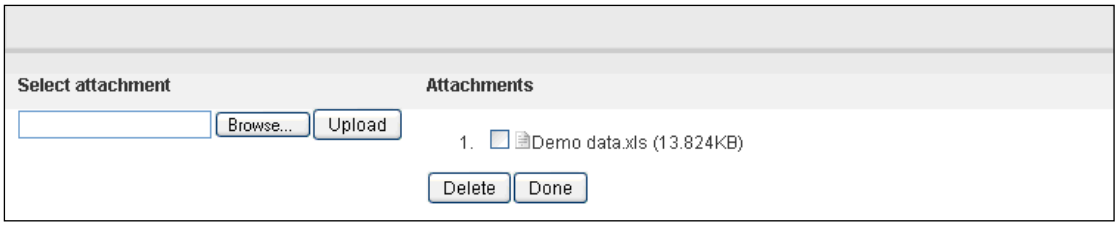

Figure 14

14. Recipient sending the encrypted reply

The attachment added from Section 13 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.

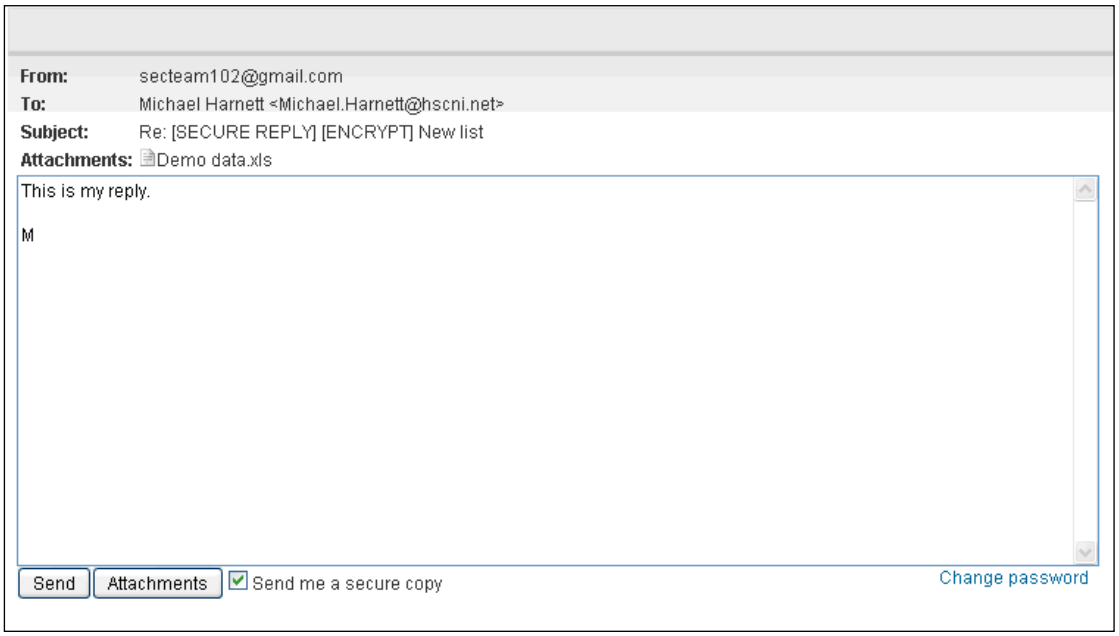

Figure 15

15. Recipient receives sent confirmation

The Recipient will receive a confirmation window if the message is sent successfully – see Figure 16.

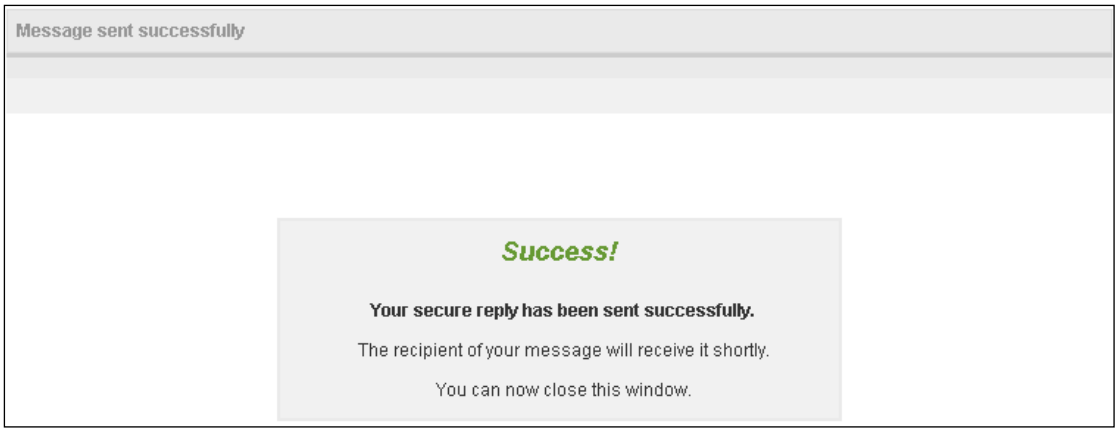

Figure 16

16. 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 17.

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.

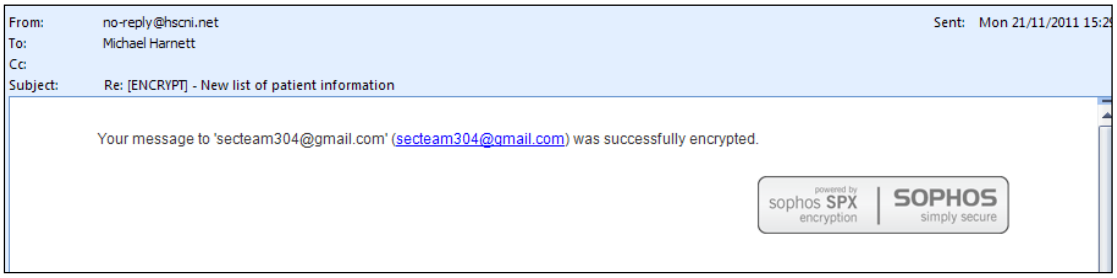

Figure 17

17. 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 18.

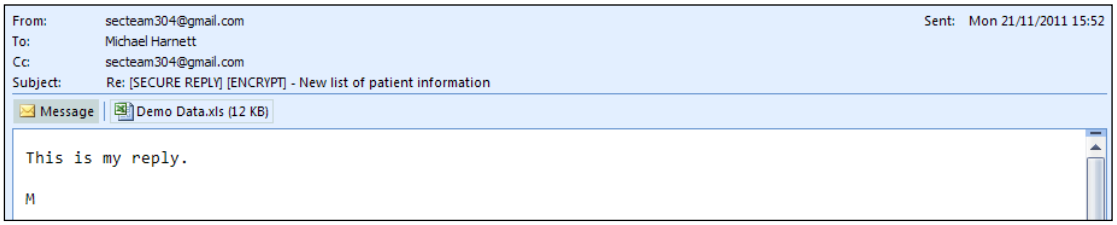

Figure 18

18. Recipient resetting the password

If a Recipient believes their password to be compromised they can reset it using the appropriate link from a previously received encrypted email from the HSC Secure Email Service.

The links are found in the body of email – see Figure 19

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 19

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 20.

Figure 20

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 21.

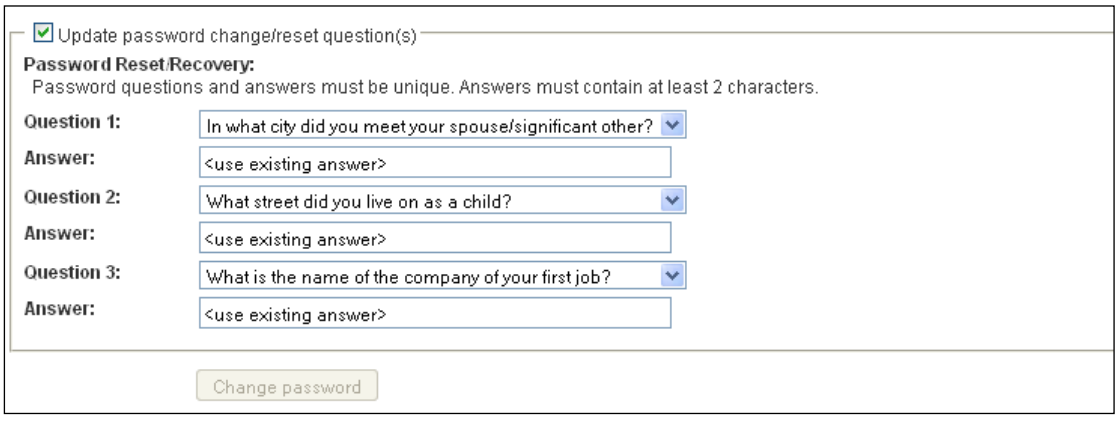

Figure 21

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 22.

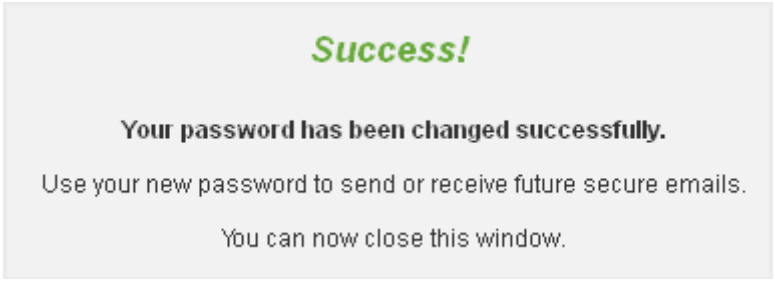

Figure 22

19. 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 HSC Secure Email Service.

The links are found in the body of email – see Figure 23

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

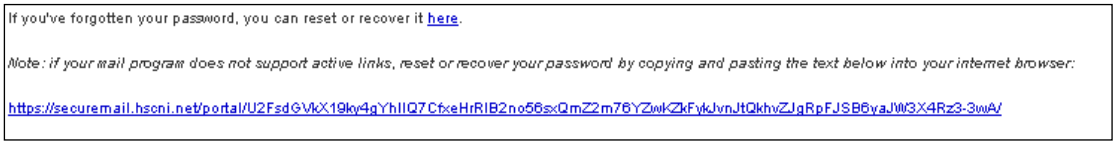

Figure 23

The following window will open in the default internet browser – see Figure 24.

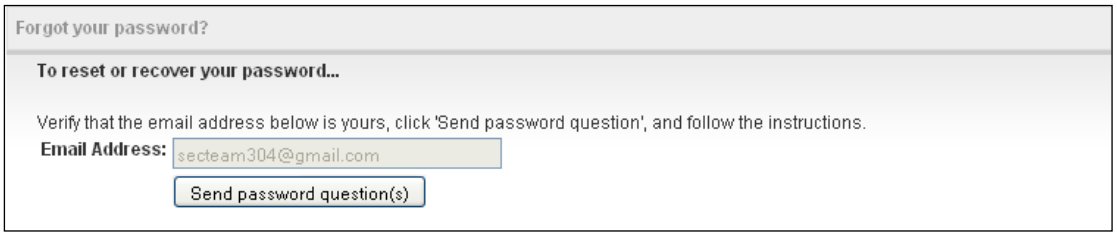

Figure 24

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 25.

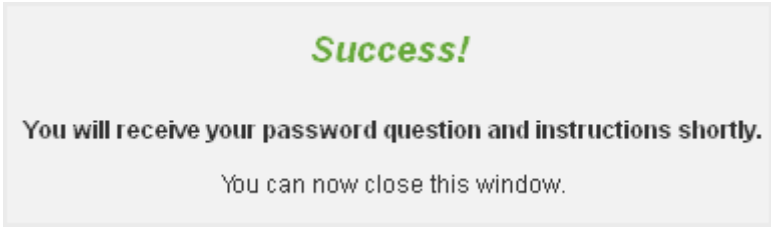

Figure 25

The Recipient will receive an email with a link to preset questions – see Figure 26.

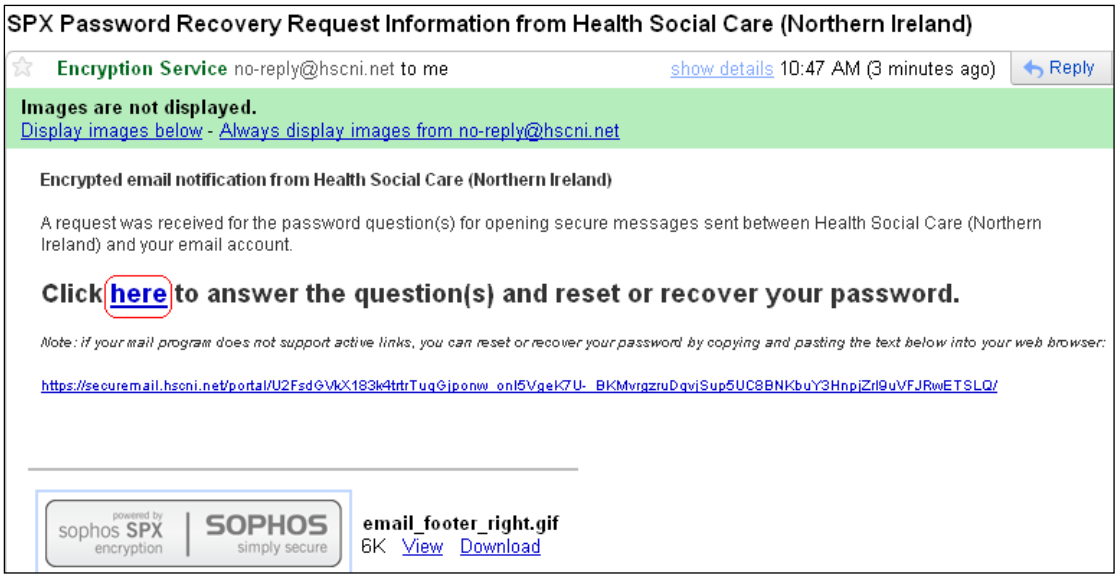

Figure 26

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 27.

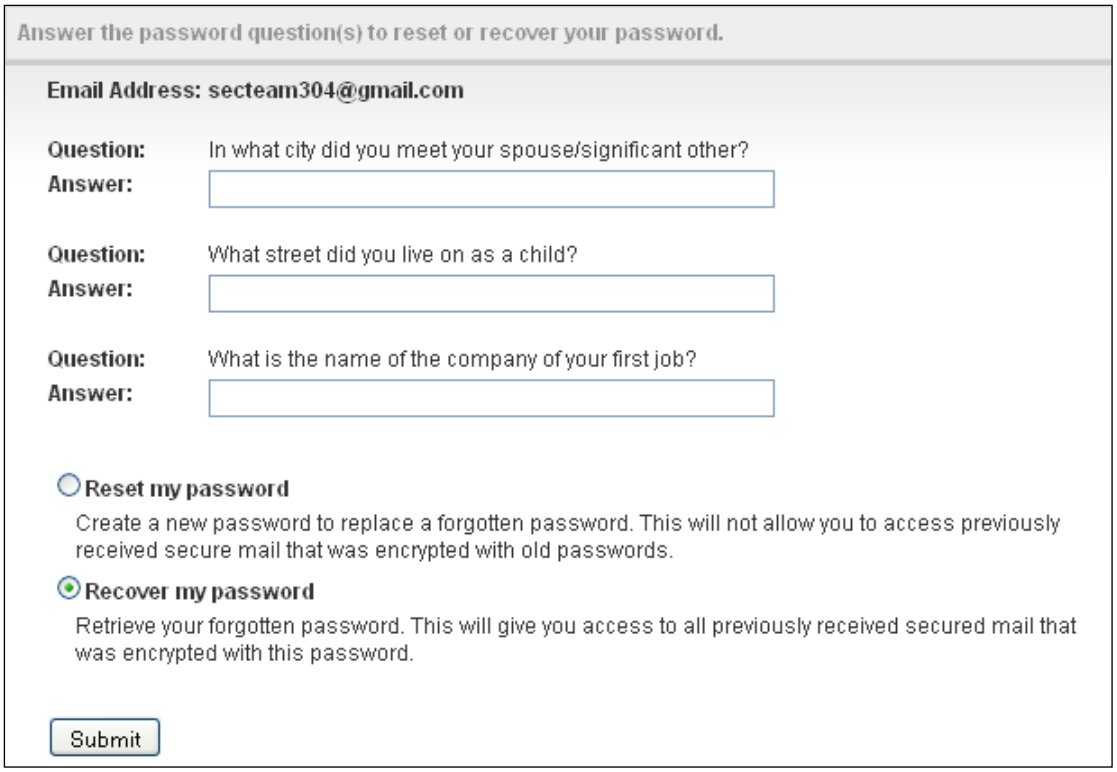

Figure 27

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 28.

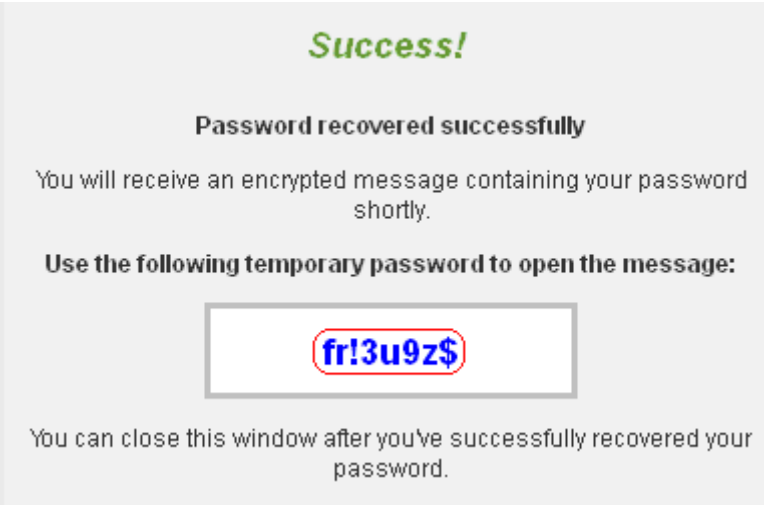

Figure 28

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 7 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.

When the Recipient cannot recall the password and the password questions, the password enrolment process can be re-initiated by the BSO-ITS Security Team. The Recipient should log a request with the BSO ICT Service Desk (see Section 20 for details). The Recipient will then receive a new SPX email that will allow them to register again.

20. Expiration Dates for Emails and Accounts

After 90 days unused Recipient accounts/passwords will be deleted. The Recipient will need to register again for any new email they receive.

After 90 days the Recipient will not be able to make a secure response. A new encrypted email will need to be sent from the Sender.

After 15 days the email will be deleted if the Recipient has not registered. A notification is forwarded to the Sender informing them of this. A new encrypted email will need to be sent from the Sender if needed.

21. Who to contact if there are problems

If you are experiencing issues or have any queries about the HSC Secure Email Service you should contact the **BSO ICT Service Desk** (Tel: 028 9536 2400 Email: supportteam@hsci.net).