Procedures for Handling Live Data

1 Objectives

- To ensure that we meet the requirements of the Data Protection Act regarding the security of customer data.
- To ensure that the confidentiality of patient information is respected.
- To ensure that the use of customer data can be audited.

2 Scope

The scope of this procedure is to detail the processes that all SCI staff **must** follow when carrying out any investigations involving backups of **live** data, from receipt of the data through to destruction or return of the data when it is no longer required.

3 Administration

The overall responsibility for all data investigations lies with the Product Support Manager. The SCI Project Officer will be designated SCI Data Investigation Administrator with the specific remit to ensure that the procedures for handling confidential data are adhered to at all times and a full audit trail is maintained. One of the Product Support team and the Product Support Manager will be designated as deputies. The nominated staff will be listed in the Data Investigation Log and a copy of the list will be made available to all SCI staff.

The audit trail will be the Helpdesk call, relating to the problem for which the data is being investigated, Test Track Number, if appropriate, and the Data Investigation Log maintained by the SCI Data Investigation Administrator.

4 Request for Data

A backup of data should only be requested from a customer for a specific purpose and as a last resort, following attempts to resolve the problem by remote support and on-site support.

A call must be logged on the Helpdesk when the request is made, clearly recording the reason for the request.

The Helpdesk must alert the SCI Data Investigation Administrator to the fact that a request has been raised and the Administrator must make an entry in the Data Investigation Log.

Customers should be requested to provide, for signature, their data protection form for releasing data. This form may be e-mailed or faxed and once signed by the requesting member of the SCI team be returned by FAX. This should be done before data leaves the customer's site.

Some customers may not have forms and be willing to release data without signature. If that is the case, this should be noted in the Data Investigation Log.

Customers should be instructed to place the data, plus a Submission note, (form available on the SCI Support website) containing the Helpdesk call number, the name of the person requesting the data and return/disposal instructions, in an appropriate protective envelope labelled "MEDICAL–IN-CONFIDENCE, F.A.O. SCI Data Investigation Administrator, Seaforth House, Seaforth Road, Hillington, Glasgow G52 4SQ".

This envelope should then be placed inside another one addressed to "GPASS/SCI Admin. Office, Seaforth House, Seaforth Road, Hillington, Glasgow G52 4SQ".

A message stating "If undelivered please return unopened to….." should be added to both envelopes.

The data must be sent by registered mail or by an alternative secure method **.

Additional levels of security should be considered, e.g. password protected zip files.

(**It is intended to include the ability to transfer data by secure electronic means once a standard has been established)

5 Receipt of Data

Whilst the data backup should be specifically addressed to the SCI Data Investigation Administrator, any backups received elsewhere must be passed to the Administrator, who will ensure the following actions are carried out.

- Check that there is an accompanying note indicating the Helpdesk Call Number and the name of the person who requested the data and file in the Data Investigation Log
  (If the note is missing, the sender should be contacted immediately to ascertain the reason for the submission of the data.)
- File the Submission note in the Data Investigation Log and retain for one month following the return/destroyal of the data.
- Log the data's arrival against the request entry in the Data Investigation Log.
  (If there is no request entry in the Log, check the Helpdesk call notes.
  If it records the request of a data backup, an entry should be made retrospectively in the Log with a note stating that it is retrospective.
  If there is no request recorded, the person named on the accompanying note should be contacted to ascertain the reason for the submission of the data, an entry should be made retrospectively in the Log, with a note stating that it is retrospective, and the Helpdesk call notes updated to include the request of data and the reason why.)
- Store the data in a secure area (to be identified)
- Update the Helpdesk call notes to record the receipt of the data.
- Inform the Product Support Manager that the clock should be restarted if it has been stopped pending receipt of the data.
- Notify the individual who requested the data that it has arrived (their name should have been supplied with the data and also should be recorded on the Helpdesk call)
- Obtain a signature in the Log from the individual accepting responsibility for the confidentiality of the data
- Pass the data to the DBA or deputy for loading on server TAZ, access to which is limited to the Product Support team and the DBA.

6 During the Investigation

If, during the investigation, there is requirement to involve another team, the Log should be updated to reflect this fact and the team leader should sign to accept responsibility.

If there is a need to have the data loaded on to another server, this fact should be recorded and the data loaded by the DBA.

At the end of the investigation, responsibility should be returned to the SCI Product Support team.

7 Removal of Data

When the investigation has been completed, the data on server TAZ, and on any other server required during the investigation, will be removed by the DBA and the Data Investigation Log signed and updated accordingly.

The original media must then be returned to the customer by registered mail or destroyed, provided there has been written authorisation from the customer. A note must be added to the helpdesk call confirming that it has been returned or destroyed.

8 Responsibilities

SCI Product Support Manager

The SCI Product Support Manager has overall responsibility for all investigations using live data.

SCI Data Investigation Administrator

The Data Investigation Administrator is responsible for the administration of this procedure, specifically the tasks outlined in para. 1.6 and in addition

- Review the Log weekly identifying
    - any datasets where the data has not been removed but the original media has been returned
    - any datasets requested that have not been received after three days and contact the customer to determine the situation.
    - any datasets that have not been returned within two weeks and ask the individual responsible for the data at that point to contact the customer to provide an update on progress.
    - Return the original data to the customer if requested and noting this fact in the Log and the Helpdesk call.

Staff Requesting Backups

Staff requesting backups must

- Confirm the need for the request with the Product Support Manager or deputy
- Inform the customer exactly why the data is needed.
- Ask the customer to FAX their relevant confidentiality form for requesting patient data.
- Sign the form and return by FAX filing copy with the Data Investigation Log.
- Ask them to send the data registered post, addressed as detailed in para 4. above, and containing a note detailing the Helpdesk call number, the name of the person requesting the data and return/disposal instructions.
- Update the Helpdesk call when the request is made, clearly recording the reason for the request.

Staff Receiving Backups

All data backups must be passed to the SCI Data Investigation Administrator irrespective of the name on the address.

Staff Responsible for Carrying out Data Investigations

All staff carrying out data investigations must ensure that the data is accessible only to those staff taking part in the investigation. If the responsibility for tracing the problem passes to another team, then the ownership of the data will pass to them and this transfer must be recorded in the Data Investigation Log. If there is a requirement for the data to be loaded on another server in addition to TAZ, this fact must be recorded in the Log.

Database Administrator

The DBA will be responsible for loading and removing the data on all the SCI servers and if requested the destroyal of the original data. The fact that the data has been removed and destroyed, if requested, must be recorded in the Log and on the Helpdesk call.

Scottish Care Information (SCI)

Common Services Agency

SUBMISSION OF DATA FOR INVESTIGATION

Please note the only purpose for which your live data will be used is to resolve the problems that you have encountered with the SCI software.

The provision of personal information on this form is for the purpose of securely tracking progress of your data while on SCI premises.

Helpdesk Call No.		**Helpdesk ID.**	
Senders Name		**Tele. No.**	
Organisation			
SCI Staff Requesting Data			
Customer Confidentiality Form Signed?	**YES / NO**	**Signed By**	
Return/Disposal Instructions	**RETURN / DESTROY**		
If data is to be destroyed			
Signature of Authorising Manager		**Date**	
Signature of Sender		**Date**	

*NB *it is intended to post this form on the SCI Support website*

DATA INVESTIGATIONS LOG

Entry	Requested		Helpdesk	Customer / Comment	Date	Person	Disposal	Data Removed		Disposal (Destroy or Return)		
No.	Date	By	Call No		Recv'd	Responsible	Instruction	Date	By		Date	By
001	14/8	XX	12390	A.N.Yone, The A Hospital	23/8	AA	Return	30/8	AB	Return	30/8	PP
	28/8			Passed to development Data to be loaded on XXXXXXX	28/8	SS	Return to Prod Supp	30/8	AB			
	29/8			Returned to Prod Support	29/8	TT						
002	16/8	XX	13987	XYZ Surgery, Anytown	19/8	TT	Destroy	23/8	AB	Destroy	23/8	AB

*** This is for illustrative purposes only. Note however as signatures are required there must be a paper based version of the log.*