SCOTTISH EXECUTIVE

Health Department

From the Chief Medical Officer

Dr E M Armstrong
FRCS (Ed) FRCP(Glas, Ed) FRCGP FFPH

St. Andrew's House
Edinburgh EH1 3DG
Telephone 0131-244-2264
Fax 0131-244-3477
e-mail: cmo@scotland.gsi.gov.uk

8th April 2004

SEHD/CMO(2004)6

For action

NHS Board Operating Division Chief Executives
NHS Board Operating Division Medical Directors
NHS Board IM&T Leads
NHS Board Caldicott Guardians
NHS ECCI Project Managers

For information

NHS Board Data Protection Officers
NHS Board Complaints Officers

Clinical Enquiries to:
Local Caldicott Guardian

Further enquiries:
Kirsty MacLeod
Basement Rear
St Andrew's House
EDINBURGH EH1 3DG
Tel: 0131-244 2351
Fax: 0131-244 5063

Dear Colleague

NHSScotland 'Best Practice' Guidance on Developing an Access Protocol for Electronic Laboratory & Radiology Result Reports in SCI Store

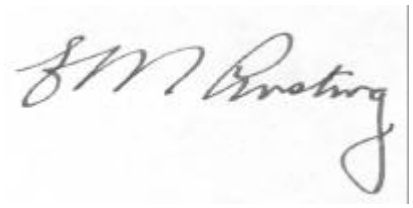
The attached document has been updated following the recent changes within NHS Health Board structures.

The document outlines 'best practice' requirements for safe and secure electronic access to diagnostic laboratory and radiology results information within NHSScotland. The document assumes that SCI Store is the clinical data repository currently in use by the Health Board to provide e-results access, and it should be viewed as the standard to which all NHSScotland organisations will aspire in respect of the treatment of personally identifiable e-results information.

The standards and practice covered by the attached guidance will continue to change both in line with different types of information being added to, and advances in the technological capabilities of SCI Store. Therefore, the document in addition sets-out how the guidance will be monitored and reviewed.

From the date of this letter, all NHSScotland Health Boards utilising SCI Store for e-results are required to update their local SCI Store Access Protocol to include the amendments set-out in the attached 'best practice' guidance.

Yours sincerely



DR E M ARMSTRONG

SCOTTISH EXECUTIVE

Health Department
Directorate of Performance Management & Finance

St Andrew's House
Regent Road
Edinburgh EH1 3DG

NHS Scotland '*Best Practice*' Guidance on Developing an Access Protocol to Electronic Laboratory & Radiology Result Reports in SCI Store

Prepared in collaboration with:

the

NHSScotland National ECCI & SCI IM&T Programmes

Version: Revised
Status: Revised Version
Date: 5th April 2004

Contents

Page

1. **Introduction**
1.1 Purpose
1.2 Policy Context 4
1.3 Local Policy 4
1.4 Scope 4
1.5 Exclusions 5
1.6 Development Process 5

2. Objectives 6
2.1 The Best Practice Guidance..... 6
2.2 This Document 6

3. General Principles 6

4. Legislation 7

5. Managing Patient Confidentiality
(see also appendix A) 7

6. Procedures for Protecting Patient Information
(see also appendix B) 8

7. Laboratory Investigations, Legislation & Definitions
7.1 Legislation – Statutory Restrictions on Passing on Information 8
7.2 Definitions of Laboratory Investigations 8
7.3 Radiology Results..... 9

8. SCI Store Access and Security Procedures
8.1 Security 9
8.2 Terms of Access to e-Results 9
8.3 Role-Based Access 10
8.4 User Registration 10
8.5 User Account Management 10
8.6 Authentication of Users..... 11
8.7 User Training 11
8.8 Environmental Security 12
8.9 Procedure for Revocation of Access Permissions 12

9. Procedure for Authorisation to input Result data to SCI Store 12
9.1 Procedure for Authorisation to Amend Result data in SCI Store 12
9.2 Retention of Patient e-Results Information..... 12

10. General Procedure for Authorising Access Permissions 13
10.1 Authorising & Managing Itinerant Locums..... 13
10.2 Authorising & Managing Agency Nurse Access to SCI Store 14
10.3 Authorising & Managing Non-Clinical Staff Access to in SCI Store 14

11. Audit Mechanisms 14

12. Protocol Management Procedures
12.1 Formal approval and adoption 15
12.2 Dissemination/Circulation of guidance 15
12.3 Monitoring and reviewing procedure 15
12.4 Reporting Breeches 16

Contents/Cont./

Page

APPENDICES

Appendix A	Must Do – Check List …….	17
Appendix B	Managing Patient Confidentiality…… …….	18
Appendix C	Protecting Patient Information ……. ……..……..	20
Appendix D	SCI Store User Registration Form…….	21
Appendix E	Partnership Agreement……	22
Appendix F	Acknowledgements & Glossary……..	28
Appendix G	References ……..…….. ……..	29
Appendix H	Example Matrix ……	30

1. Introduction

This document outlines 'best practice' requirements for safe and secure electronic access to diagnostic laboratory result information within NHS Scotland. It should be viewed as a means of establishing a standard to which all NHS Scotland organisations will aspire in respect of the treatment of personally identifiable electronic results information. There is an underlying assumption that SCI Store is the clinical data repository currently in use by the Health Board for providing access to electronic results reporting or will be in the near future.

This is an evolving document because the standards and practice covered will continue to change both in line with different types of information being added to, and advances in the technological capabilities of SCI Store. Where appropriate, it is supplemented by additional guidance on the SHOW web site http://www.show.scot.nhs.uk/confidentiality.

1.1 Purpose

To establish common core 'best practice' guidance which will form a core protocol for the management of access permissions to all e-results in SCI Store.

1.2 Policy Context

The aim of recent government policy is that patients receive the services/treatment that they need from NHS organisations in a fast, efficient and personalised manner. In order to achieve this the NHS Executive has both embarked on a modernisation programme, and set out a robust IM&T strategy to deliver a health service fit for the 21st Century. A key component of this strategy is ensuring that those involved in delivering the '*frontline*' healthcare services have the information they need to provide co-ordinated, seamless care to patients. Their needs for information cannot be met easily without electronic medical records and other computerised systems.

Without access to appropriate information, a health system is at best inefficient and frustrating and at worst dangerous.

1.3 Local Context

NHS Scotland is in the midst of ambitious modernisation. New computer-based information systems will improve the delivery of care by ensuring the right information is in the right place at the right time. SCI Store is one of a suite of key national IT products being developed to achieve this goal. It is envisaged that SCI Store will form a major part of the future *Integrated Care Record* (ICR), providing access to patients' diagnostic laboratory investigations, GP referral and Hospital discharge letters and GP summary data.

At present SCI Store is being rolled out across NHS Scotland to provide both Primary and Secondary care clinicians with timely access to patient diagnostic laboratory test results. The ability to share such information more efficiently potentially offers great benefits – better health care, fewer lost records, more efficiently run GP Practices and Hospitals, shorter waits for treatment, research leading to new treatments, fewer medical errors and better protection of public health.

Nevertheless, more efficient sharing of health information also presents some risks. As medicine develops, more will be known not only about people's present health but also about their future health. If, for example, this information is inappropriately shared outside the NHS it may prejudice people's ability to get jobs, life insurance or mortgages. One way to minimise the risk is to have informed patients exercising as much control as possible over who sees their medical information. Yet, safeguards must not create impossible barriers to information sharing for good care**.**

1.4. Scope

This protocol covers the accessing of e-results information in SCI Store for any of the purposes listed below and comprises common principles and procedures that must be adopted whenever NHSScotland

organisations provide employees and independent contractors access to e-results for these purposes. These are:

- Direct Patient Care
- Security Audit
- Organisational Management Information

1.5 Exclusions

In due course separate protocols will be developed to manage Public Health Consultants access to SCI Store for example for - for communicable diseases, tertiary centres outwith NHS Board, cancer management centres, MCN, and Cancer Registries. Research project access to SCI Store data will also be dealt with under a separate protocol.

1.6 Developmental Process

The main driver behind the development of this 'best practice' guidance has been the differing clinical views around access permissions and management of patient confidentiality encountered by the Electronic Clinical Communication Implementation Project (ECCI) Project Managers across NHS Scotland while implementing SCI Store for e-Results Reporting.

An initial consultation exercise was conducted by the ECCI Central Team on 2nd September 2003 with Senior Laboratory Personnel, ECCI Project Managers, SCI Team, and Data Protection Officers from across NHS Scotland. A small sub-group was formed as a result of this consultation exercise to further refine the structure and content of this 'best practice' guidance document.

The approach taken to the development of the guidance was first to:

i) Recognise the good practice already in place regarding clinical and non clinical staff access to manual records (case notes/paper results) and/or electronic lab results.
ii) Acknowledge dependency – that access protocols rely on a combination of organisational policy/procedures, whole system processes and IT systems that provide security and access control facilities.
iii) Realise individuals statutory responsibilities (e.g. clinicians/non-clinicians professional codes of conduct governing the management of patient confidentiality)
iv) Utilise NHSScotland IT system security standards, where appropriate
v) Assimilate all of the above into the best practice guidance

This document was also informed by:

- NHS Scotland Code of Practice on Protecting Confidentiality (NHSScotland July 2003)
- Department of Health Confidentiality Code of Practice (DOH July 2003);
- NHS Information Authority 'Caring for Information – Model for the Future' (NHSIA October 2002);
- Share with Care – NHSIA & Consumers Association 'Peoples views on Consent and Confidentiality of Patient Information' (October 2002)
- Gaining Patient Consent to Disclosure (NHS Executive January 2001) (for full references see appendix)
- Consultation with SEHD DCMO Dr. Andrew Fraser & Dr. F Bisset SEHD Caldicott Advisor

2 Objectives

2.1 Best Practice Guidance

1. To provide a robust framework for the legal, secure and confidential access to personal electronic diagnostic laboratory test result information within NHS Scotland Health Board organisations, to enable clinicians to meet their professional obligations and deliver appropriate, timely healthcare advice and treatment to patients.

2. To define the purposes for which e-Results information will be used (see 1.3)

3. To define the roles and responsibilities of those involved in the operation of this guidance

4. To inform patients of the NHS Scotland organisations who are party to this best practice guidance of the reasons why their diagnostic laboratory results information may be viewed electronically and how this electronic accessing will be controlled and managed.

.

In respect of diagnostic laboratory tests, a **'Clinician'** is a health care professional responsible for delivering advice or treatment to a patient based on the results of their laboratory investigations, e.g. doctors, nurses, laboratory scientists, physiotherapist, dieticians and pharmacists. There will also be times when non-clinicians e.g. SCI Store System Administrator or Consultants & GP Practice Secretaries/Administrative staff may need access to patient's laboratory investigations e.g. creating new user accounts or for the purpose of writing patient referral/discharge letters or managing incoming test results.

2.2 This Document

i) Establishes the principles under which the best practice guidance will operate
ii) Sets out the legal and ethical obligations that underpin the management of patient e-information
iii) Describes the processes that must be in place to inform patients effectively of how their e-results information will be used and disclosed in line with statutory responsibilities and patient choice
iv) Describes the structures that must be in place to protect patient information
v) Outlines the statutory legislation that must be taken into consideration when providing access to laboratory investigations and clarify the distinction between 'highly sensitive' and sensitive laboratory results.
vi) Describes the Security, Terms of Access to e-Results in SCI Store, Role-Based Access, Registration, User Account Management & Authentication Processes, and Training requirements.
vii) Illustrates an Authorisation procedure to Input data into SCI Store and the process for the management of amending test report data in Store.
viii) Illustrates a General Authorisation procedure for granting Access to SCI Store
ix) Outlines the Audit procedures that are required to be in place
x) Sets out how the protocol will be implemented, monitored and reviewed

3. General Principles

The general principles under which this document operates are as follows:

i) e-Results information will only be accessed by the NHSScotland employees described in this protocol
ii) Access to patient identifiable electronic results will only be provided for delivery of health care as described and agreed in this document
iii) Clinicians will only access the information they need to know to do their job in caring for the patient
iv) Use of electronic results data for purposes other than direct patient care will be anonymised whenever possible.
v) The maintenance, monitoring and review of this guidance will be the responsibility of SEHD, SCI Store e-Results Best Practice Guidance Sub Group. These individuals will perform the duties of Protocol Guidance Guardians.

4. Legislation

The key objective is that the handling of patient identifiable information by NHSScotland conforms to all applicable law. Protection of personal health information is part of good clinical practice, and is underpinned by the Common Law duty of Confidentiality, and the Access to Health Records Act 1990 (for deceased persons records). The key legislation governing the protection and use of identifiable patient information has been the Data Protection Act 1998 (DPA98), and the new Human Rights Act 1998. Arrangements for use of Personal Health Information should meet these requirements. A guide to the Data Protection Act is available at **http://www.dataprotection.gov.uk**

In addition to the above mentioned legislation, consideration may also need to be given to the following:

i) The CSAGS Final Report 2001 **http://www.show.scot.nhs.uk/csags/**
ii) The Caldicott Committee Report 1997 **http://www.doh.gov.uk/ipu/confiden/report/**
iii) The Crime & Disorder Act 1998 (Section 115) **http://www.hmso.gov.uk/acts1998/19980037.htm**

There are also revised Codes of Professional Practices, and ministerial guidance from the Scottish Executive Health Department such as HDL (2003) 37 to help health professionals comply with legislation http://www.show.scot.nhs.uk/sehd/.

Patient information is generally held under legal and ethical obligations of confidentiality within the healthcare team. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule (see http://www.show.scot.nhs.uk/confidentiality).

A specific requirement of the Data Protection Act 1998 is that patients need to be informed of the identity of the 'data controller' and the purpose to which their data will be put. The data controller is the organisation that determines how and for what purposes, patient identifiable information is collected, held and processed. At present the data controller responsible for Personal Health Information generally rests with the Director of Public Health for an NHS Board, but in a small number of cases this role is fulfilled by either the senior designated doctor or nurse (Medical Director/Director of Nursing). Within the Primary Care division of NHS Boards the General Practitioners (GPs) are the data controllers.

The DPA also requires organisations to use the minimum amount of information on a '**NEED TO KNOW'** basis.

***"Need to know"* is interpreted as meaning that members of an organisation should have access to information if the function or role which they are charged with fulfilling at that particular point in time in relation to a particular person, cannot be achieved without access to the information specified.**

Advice on any data protection issues relating to SCI Store and e-Results reporting, in the first instance, should be directed to the local Health Board/Trust Caldicott Guardian. If there are concerns over the way to proceed on a particular issue the local Caldicott Guardian can seek further guidance from the SEHD Caldicott advisor.

5 Managing Patient Confidentiality

Within NHSScotland there is a lot of very relevant good practice documentation available on the management of patient confidentiality (http://www.show.scot.nhs.uk/confidentiality & http://www.show.scot.nhs.uk/csags). These papers informed the development of the *'best practice'* guidance on e-results and managing patient confidentiality set-out in appendix B. The guidance material includes:

i) Informing Patients – Effectively
ii) Patient Access
iii) Patient Choice - Consent
iv) Patient Refusing or Restricting Disclosure
v) Managing Disclosure Without Consent

6 Protecting Patient e-Results Information

Access Protocols do not stand alone. They are part of managerial policies and procedures which in combination with robust IT security practices and standards serve to protect patient confidentiality. This dependency must be acknowledged when considering the procedures necessary for protecting patient e-results information. In order to protect patient e–results information a SCI Store Access Protocol is dependent upon:

i) Confidentiality being a contractual obligation for all NHS Scotland staff
ii) NHSScotland staff knowing their obligations
iii) Accuracy & Consistency in Recording Patient Information
iii) NHSScotland staff keeping Patient e-Information Private

These policies and procedures are described in more detail in appendix C.

7. Laboratory Investigations, Legislation & Definitions

7.1 Legislation – Statutory Restrictions on Passing on Information

There are three areas of legislation where specific statutory restrictions on disclosure of information apply:

i) The Human Fertilisation & Embryology Act 1990 amended under The Human Fertilisation and Embryology Act 1992 limits the circumstances in which information may be disclosed by centres licensed under the Act.
ii) The NHS Venereal Diseases Regulations 1974 and the NHS Trusts Venereal Diseases Directions 1991prevent the disclosure of any identifying information about a patient with a venereal disease other than to a medical practitioner under specified circumstances.
iii) The Abortions Regulations 1991 limits and define the circumstances in which information submitted under the Act may be disclosed (places restrictions on the DPH and will apply to very few electronic systems).

It is likely that SCI Store may hold some information that falls under these categories. Therefore agreement for release of such information from laboratories to SCI Store must be controlled by the requesting location e.g. GUM, GP, or by specific 'test type' e.g. HFEA and VDR patients are identified by a secondary code. Controlling the information flows at source removes the issue.

Nevertheless, there are two options for managing data falling under the above statutory legislation:

i) Manage in Laboratory System and not release the data to SCI Store
ii) Release data from lab system to SCI Store and control access by requesting location

While option (ii) is ultimately the preferred route, there is additional administrative management involved for the local SCI Store System Administrator/Technical support staff. Therefore the method chosen must be a local clinical decision.

7.2 Definitions of Diagnostic Laboratory Information

Results in the laboratory systems are generally conceptually categorised as "highly sensitive" requiring particularly stringent safeguards on disclosure or "sensitive" including most clinical laboratory data.

Highly sensitive pertains to *'all personal results where the patient wishes disclosure restricted to a defined minimum (less than for sensitive results) and/or where the patient has to be counselled before the test is taken'.* For example see list below:

- GUM clinic sexual health tests
- HIV
- Hepatitis B & C

- Occupational health lab tests
- Drug addiction clinic tests
- Pregnancy Tests (limit access to requesting location)

Sensitive results pertains to all other clinical laboratory investigations e.g. full blood count, urea and electrolytes.

Electronic access to 'highly sensitive' test results for the purposes of direct patient care must be restricted to the requesting location. The options for the management of 'highly sensitive results' are the same as those described above under section 7.1 statutory regulations. Again, while option (ii) is ultimately the preferred route and the long term goal, the method chosen must be a local 'clinical' decision.

It is also important to stress to requesters of laboratory investigations the need to be *careful* over what information they write on test request forms (e.g. sensitive information such as ?HIV), as it is very likely that this information will appear back on the e-result report.

.

7.3 Radiology Reports

Written descriptive Radiology reports (not images) can be made available in SCI Store. Examples of these reports include the results of a GP request for X-ray, Ultrasound Scan and/or Medical Physics Report. PACS system will deliver e-Radiology image reports in the future.

It is recommended that all Radiology reports should be verified before release to SCI Store. But, it is also recognised that there are circumstances where it may be necessary to release unverified Radiology reports. Therefore, the approach taken to the management of the release of Radiology reports to SCI Store must be a local clinical decision. Unverified radiology reports must be clearly identified as unverified.

8 SCI Store Access and Security Procedures

8.1 Security

SCI Store provides secure access control (see 8.3 and 8.6) and audit trail facilities (see section 11) which support an organisation in satisfying The Data Protection Act 1998 and ISO 17799:2000 (where applicable). Users have web browser access to SCI Store which utilises Microsoft's IIS (Internet information services) supports HTTPS (Secure HyperText Transfer Protocol) with SSL (Secure Socket Level), providing digital certificates and 128 bit public key encryption. WAN (Wide Area Network) access is across a private, secure NHSnet network connection or internal network accredited to connect to NHSnet.

8.2 Terms of Access to E-Results

Information on SCI Store must only be accessed on a genuine 'need to know' basis. This requires that those who use a patient's information:

i) Are who they claim to be through authorisation identity checks
ii) Have a legitimate care relationship with the patient
iii) Only see information their role allows

An audit trail record is kept of everyone who views a patient's e-results record.

8.3 Role-Based Access, & Controls

Role based access provides a manageable, scalable approach to access control which is sufficiently flexible to cater for early implementation. A user of SCI Store will have one or more user access role/s, each of which they are assigned and carry out on behalf of the GP Practices, Trust/Health Board they work in (e.g. GP, Midwife). Each user role will group together users (work groups) with a common set of access privileges. In other words each user access role will provide a set of users with general access to the same types of data. Two users with the same role may be entitled to access data about different sets of patients.

Each NHS Board must identify their SCI Store data controller/s who will approve the 'rules' for access to data in SCI Store. In particular the SCI Store data controller needs to agree user role classifications and access rights for each user role with the appropriate clinical directors/line managers. Steps in this process must include:

i) Identify the roles where there is a legitimate 'need to know' interest in gaining access to e-results information
ii) Agree the level of confidentiality for this class of information
iii) Identify the reasons which justify giving access to a particular level of information
iv) Complete a matrix showing the access available for each role and the reason why access is justified (example in appendix H)

For each SCI Store implementation there must be a designated SCI Store System Administrator whose job will include setting up approved user accounts and access controls.

8.4 Registration of Users

Access to SCI Store health information must be subject to a formal user registration process, an example of a standard SCI Store user registration document can be located at appendix D. User registration procedures must ensure that the level of user identification that is provided is consistent with the level of access that will become available to the user. The SCI Store System Administrator must only create a user account on receipt of a properly completed request form. All user registration details must be periodically reviewed to ensure that they are complete, accurate and that access is still required.

8.5 Management of User Accounts

Management of user accounts is **not** the sole responsibility of the SCI Store System Administrator. Maintenance of accurate user account information is the 'joint/shared' responsibility of the individual user, the authority that granted that users access (i.e. clinical line manager) and the SCI Store Administrator. The method employed to manage SCI Store User Accounts is a local decision, but it must clearly define roles and responsibilities. Two examples of effective user account management processes are described below:

1. The use of a 'Partnership Agreement' between Laboratory Services and GP Practices/OOH/Hospital departments is a very good method of establishing at the outset the 'joint/shared responsibility' for managing user account details. An example of a Partnership agreement can be located in appendix E. Apart from outlining the quality of information expected on test requests entering the Lab, the Partnership Agreement should address the local process/es for adding/deleting and maintaining user registration Details (including Human Resource Department involvement). That is, clearly describing the roles and responsibilities of all those party to the agreement in maintaining accurate user account information.

2. Every 3 months the SCI Store System Administrator runs a SQL query in SCI Store to identify which users have not accessed the facility in the past 3 months and remove/delete their access permissions following appropriate liason with departments.

In **Primary Care** it is recommended that a practice management contact in each GP Practice is given a list of accounts relating to their practice on a 6 monthly basis to review and up-date. The list should be checked, amended and returned promptly to the SCI Store System Administrator. Delay in return of this information to the System Administrator should lead to practice access to SCI Store being switched off, although, ultimately

this is a local decision. Community Nurses and AHP's access to SCI Store should be included in this management process.

It is also recommended that a similar process to that described for GP Practices be applied to the management of User Accounts for **Out of Hours Services**.

In the **Acute Hospital** setting each site must have a robust system for the management of user registration processes, in particular new starts and leavers. This system must involve the Human Resource department in each Acute site and devolve the control of managing user registration to the appropriate departmental managers. The processes and documentation outlined for managing user registration in Primary Care may also be adapted for use in the Acute setting.

8.6 Authentication of Users

Access to the electronic results reporting facility must be controlled by a *'unique user name and password'* system that meets the minimum NHSScotland Standard (see http://www.show.scot.nhs.uk/security). Password management must comply with the specifications set out in volume 3 NHSScotland Security Manual (http://www.show.scot.nhs.uk/security), also see section 6.4 appendix C protecting patient information. Passwords must be time limited, a renewal period is recommended at between 30-60 days.

Logging on to SCI Store is controlled by unique username and password. It is for local management to ensure that this user id is used by one and only one individual. SCI Store system allows the period between password changes to be set up locally

There is a future vision of a unique user ID across NHSScotland and an associated authentication facility that is linked directly to the NHS Directory. At present, the means by which to implement this are not yet in place.

8.7 User Training

All users must have been briefed on:

- Local User Training and Awareness materials (dummy patient details must be used during training)
- IT Security Policy
- The Computer Misuse Act
- The Data Protection Act
- NHSScotland Code of Practice on Protecting Confidentiality

It is important all IT users are made aware of their confidentiality and security responsibilities from the outset. Before any user is given access to SCI Store training must be given. This should include reminders about applicable general policies and procedures, and guidance on what may constitute inappropriate access. Initial training must also be followed-up by regular up-dates in organisational policies and procedures.

There is national CBT training on Confidentiality and Data Protection available at **http://www.show.scot.nhs.uk/elearning**

Local training documentation should clearly specify who should be contacted if a user requires assistance with the SCI Store application e.g. Local Health Board IT helpdesk (not SCI Store System Administrator).

All users must be fully informed (verbally and in writing) of their legal and ethical responsibilities in respect of data protection, and must sign a confidentiality statement prior to access being granted to the SCI Store system.

8.8 Environmental Security

Unattended workstations must be protected against an unauthorised use with an automatic timeout facility. The period of time the timeout facility is set to within SCI Store is a local decision, and should be based on local requirements. The onus here is clearly on the individual to maintain patient confidentiality, and ensure that they log-out after using the facility. This must be emphasised during user application training. Currently, re-admittance to SCI Store will require the user to re-submit his/her id and password. Re-admittance will take the user back to the original login page.

8.9 Procedure for Removal of Access Permissions

The System Administrator must be informed immediately when staff no longer have a legitimate right to access the system or leave a department. This must be conducted by the appropriate Line Manager advising the System Administrator immediately or proactively. The management of access permission of personnel leaving must comply with the requirements set out in section 4.2 of NHSScotland Security Manual (**http://www.show.scot.nhs.uk/security)**.

Violation of NHSScotland security policies and procedures by employees, agents, subcontractors of or other persons must be dealt swiftly by immediate revocation of access privileges. A formal management procedure must be in place to deal with such circumstances. The NHSScotland Security Manual provides guidance in this area (**http://www.show.scot.nhs.uk/security)**. An audit log must be kept of all breaches of local SCI Store Access Protocol. The contents of this audit log must be monitored and reviewed at regular intervals.

9. Procedure for Authorisation to input Result data to SCI Store

i) Agreement for input of data to SCI Store is provided on the authority of the SCI Store data controller/owner and the organisations Caldicott Guardian (if this role is held by a different individual)
ii) The procedure for release of authorised results data from source systems to SCI Store will be determined by the appropriate Clinical Director and/or Departmental Manager
iii) Laboratory Consultants who authorise reports, may grant discretionary access control to enter results or reports on the laboratory system that feeds SCI Store to specific work groups/lab team members working under their direct authority. These work groups may include medical, scientific, technical and administrative staff within the laboratories.

9.1 Authorisation to make Amendments to Result data in SCI Store

Amendments to test request data normally occur within the Laboratory system prior to release of the test report to SCI Store. Nevertheless, there are a few situations where amendments to fully authorised result reports released to SCI Store can be required for-example:

i) The sample is subsequently found to have been delayed in transit and therefore unsuitable for analysis
ii) The sample is subsequently found to be contaminated
iii) The result is subsequently found to be analytically incorrect
iv) The sample is subsequently found to be haemolysed, lipaemic etc
v) When the requesting clinician adds or deletes tests from the original request
vi) When the requesting clinician adds/amends clinical details/reasons for report
vii) When there has been an error in the patient or sample identification details supplied with the request

The procedure depends on the nature of the change/amendment required. If the change is critical, that is the result is incorrect and may alter clinical management now and in the future, the result must be corrected. The procedure is:

i) Where feasible, inform the test requestee and/or requesting location by telephone and explain the need for the change.

ii) De-authorise the report.
iii) Attach a suitable comment indicating the nature of the change and date of amendment.
iv) A new report should be automatically issued (this will then be released in the normal manner to SCI Store which will recognise and treat it as a replacement report).
v) Under **NO** circumstances should the incorrect record be deleted from SCI Store.
vi) The incident must be logged and reported at the appropriate local forum e.g. laboratory audit meeting, risk management, clinical governance meeting.

Laboratories should have a clear written policy and procedure for handling requests which have insufficient information to adequately uniquely identify the patient or sample.

SCI Store also provides an e-note/postit facility attachment for each test report. The person who first notes the 'inaccuracy' (i.e. Lab personnel or test requestor) in a test report may utilise this facility to append a suitable comment so that other clinicians electronically accessing the report are aware of the mistake.

9.2 Retention of Electronic Patient e-Results Information

The period of time that patient e-results information should be held in electronic format is as yet to be determined, current policy is under review and new guidance will be forth coming later this year.

10. General Procedure for Authorising Access Permissions

The Director of Public Health for the NHS Board will be ultimately responsible for approving and delegating the authority to access SCI Store. In a small number of cases this role may be fulfilled by either the senior designated doctor or nurse (Medical Director/Director of Nursing). Within the Primary Care division of NHS Boards the Lead GPs within each practice are responsible for approving access to SCI Store.

i) Access is provided on the authority of the SCI Store data controller (Director of Public Health/GP). The data controller can approve and devolve the authority to Hospital Consultant and Heads of Service/Departments (there may be some variation from one NHS Board to another).
ii) Lead GPin the Practice/ Clinical Directors, once approved, can approve all access to clinical team members (Registrars/SHO's) on a 'need to know' basis.
iii) Nurse access must be authorised by both the Senior Clinician and direct Clinical Line Manager.
iv) Locums contracted to work a set period in a GP Practice/Hospital must have authorisation to access SCI Store granted by the Lead GP/Hospital Clinician, and access should be time limited.
v) Community Pharmacists access to SCI Store must be approved by the Medical Director.
vi) PAMS/AHPs access to SCI Store must be authorised by both their Clinical Director and direct Clinical Line Manager.

10.1 Authorising & Managing Itinerant Locum Access to SCI Store

In Primary Care the Lead GP for the Practice is responsible for authorising itinerant Locums access to SCI Store. At present SCI Store does not have an account type that supports users operating over multiple sites, therefore, how itinerant locum access to SCI Store is managed must be a local decision. One pragmatic solution is for the Lead GP to authorise a small block of username and password combinations to be utilised for itinerant Locums and evolve management of them to an appropriate member of staff. All username and password combinations issued to itinerant locums **must be unique**. A mandatory requirement of authorising access to SCI Store is that there is **no re-use** of usernames and passwords. It is also good practice to keep a register within the GP Practice of which Locum worked which session on what day. Itinerant locums must receive adequate training in use of and rules governing access to the system.

For Out of Hours Services the Lead GP in the Practice is responsible for authorising itinerant locum access to SCI Store. Again, how itinerant locum access to SCI Store for OOH Services is managed is a local decision, but a similar process to that described for GP Practices would be one sensible approach.

In the Acute Hospital setting it is impractical to expect the Clinical Heads of Department/Consultants to be available to grant itinerant Locum access to SCI Store. Again, how itinerant locum access to SCI Store is managed must be a local decision. But, one practical method would be for the Clinical Director/Consultant to authorise the use of a block of usernames and passwords specifically for itinerant locums working within his/her department and devolve management of them to an appropriate member of staff. As described above for GP Practices, all username and password combinations issued to hospital itinerant locums **must be unique,** and there must be **no re-use** of usernames and passwords**.** It is also feasible to utilise specific time limited usernames and passwords, albeit that this requires increased system administrative support.
.

10.2 Authorising & Managing Agency Nurse Access to SCI Store

Access must be provided on the authority of the SCI Store data controller – and must only be granted if access and appropriate safeguards are written into the contract with the particular nursing agency. The data controller can approve and may devolve the authority to grant agency nurse access to SCI Store to the appropriate Clinical Heads of Departments. Agency nurse access to SCI Store should be managed as per itinerant locums. The decision to allow agency nurse access to SCI Store must be a local one.

10.3 Authorising & Managing Non-Clinical Staff Access to e-Results In SCI Store

Access must be provided on the authority of the SCI Store data controller. The data controller can devolve the authority to grant access to the appropriate employees direct clinical or head of services manager. Access to SCI Store data for this group will be granted strictly on a need to know basis.

NHS Non-Clinical Staff who may require access to SCI Store include:

- Consultant's/GP Secretaries – preparing patient referral/discharge letters and performing the job of supporting the consultant.
- The System Administrator/Manager will have access to add or delete users, (on instruction from a clinical authority) change passwords and to monitor access.
- Authorised technical support staff that diagnose and correct faults and ensure that system works effectively.

11. AUDIT Mechanisms

The provision of an Audit Trail is a fundamental requirement of information governance. Audit Trail enables users to be made accountable for their actions in the system, and offers a security record for use in analysing breaches of security and policy. Within SCI Store whenever e-Results data are "output" a record will be made in an audit trail. These in-built audit logs allow identification of all system users who have accessed or modified a patient record over a given period (who, what where, and when).

Audits to ensure compliance with these Terms and Conditions of local Access Protocols must be undertaken on a regular basis by suitably authorised personnel within each Trust/Health Board (i.e. SCI Store SA and user support staff). NHS organisations must be in a position to demonstrate their SCI Store audit procedures on request. Examples of good practice audits include:

Looking for atypical accessing:
- Repeated unsuccessful access attempts
- Wrongly submitting password 3 times
- Long periods worked by an individual user
- Casual Browser

Other types of audit that should be conducted from time to time at local level include:

- Retrospective analyses - take a particular hospital department on a certain day/s. Run a SQL query in Store to establish who from that department used the facility during that period, what they looked at, and whether it was appropriate (i.e. were the e-results viewed those of patient being treated in that department

on that day).

- A proactive walk around hospital audit. This is where IT security staff take a walk around hospital wards to check whether the person using the computer terminal is logged-in in their username name or some-one-else's. Staff found to be accessing SCI Store with another member of staffs username and password should be subject to the Trust/Health Board disciplinary procedures. In such circumstances the member of staff's user account should be deactivated. Only following re-training and education should the users account be reactivated.

The Maintain SCI Store document which can be located at http:www.show.scot.nhs.uk also provides proposals for good practice with regard to audit.

12. Best Practice Guidance Management Procedures

12.1 Formal approval and adoption

This document was formally approved by the Chief Medical Officerfor NHSScotland Dr. Mac Armstrong on 5th April 2004.

12.2 Dissemination/Circulation of Best Practice Guidance

The 'best practice' guidance will be disseminated to all Health Board CEO's, Trust Medical Directors, Trust Caldicot Guardians, Heads of IM&T and ECCI Project Managers for action/implementation. Copies of the 'best practice' guidance will also be circulated to all relevant NHSScotland Data Security/Privacy Officers, Complaints Officers etc.

This document is also available to download from the following web site/s:

ECCI **http://www.show.scot.nhs.uk/ecci**
SCI **http://www.show.scot.nhs.uk/sci**
SE http://www.show.scot.nhs.uk/sehd/

12.3 Monitoring & reviewing procedures

The best practice guidance will be subject to a formal yearly review.

Expert Clinical Guidance and Legal advice will always be sought before any major changes to the guidance are considered.

i) The body responsible for reviewing and agreeing changes to the guidance is the SEHD SCI Store e-Results Best Practice Guardians Sub Group.

ii) The date of the initial review is 4th December 2004.

iii) The person who will co-ordinate the review Mr. Charlie Knox, Director of IM&T, SEHD.

iv) Following the introduction of the best practice guidance, its use and application will be closely monitored until the date of the first formal review. During this period changes will only be considered if the issues and problems identified are felt to be a significant barrier to providing access to or sharing information in SCI Store.

v) The use and effectiveness of the best practice guidance will be evaluated in a number of ways:

- Following adoption of the guidance, confirmation will be requested from NHSScotland Health Boards that they have implemented the procedures as required by the guidance
- The local Caldicott Guardian/IT DPO's and Complaints Offciers for NHSScotland Health Boards will be consulted 2 months prior to the guidance review date for documentation

pertaining to breaches and issues arising form implementaiton.
- Analysis of documentation pertaining to reported breaches of the guidance.
- Analysis of complaints received by organisations to determine whether they relate to breakdown or inadequacy of the guidance

.

12.4 Reporting Breaches of the Guidance

The following types of incidents must be logged to organisational security officer:

- Disclosure of information to members of staff who do not have a legitimate reason for access to that data
- Breach of procedures
- The use of SCI Store data for purposes other than those agreed in the best practice guidance
- Inadequate security arrangements

Appendix A

Must Do - Checklist!

When Developing a Local SCI Store Access Protocol for e-Results the following points must be addressed:

1. Establish a manager to take responsibility for developing access control. Typically this will be the Project Manager.

2. In addition, identify an individual to take ongoing responsibility for oversight of access control – the Protocol Guardian. The local Caldicott Guardian may assume this responsibility or delegate it.

3. Check that the appropriate SCI Store System Security is in place, that it is operational, and meets the requirements in **sections 8.1 & 8.6** of this guidance

4. Liaise with local Senior Laboratory Clinicians, System Managers, Radiologists and DPA Officers to establish:

   a) Which test results will be made available in SCI Store (see **all of section 7)**
   b) The procedure to grant authority to input data to SCI Store (see **section 9**)
   c) The procedure for amending test result data in SCI Store (see **section 9.1**)

5. Use appropriate local consultation mechanisms to engage Senior Partners of GP Practices, local OOH Services and Clinical Heads of Departments in the Acute Trust to agree:

   a) The authorisation process for granting Access to SCI Store (see **all of section 10**)
   b) The terms and level of access to be granted to various grades of staff (see **sections 8.2& 8.3**)
   c) The Registration of Users and Management of User Accounts (see **section 8.4**)
   d) Methods of informing – patients effectively of how their e-results information is being used and obtaining express consent (see **appendix A section 5.1 & 5.2**)
   e) The management of situations where a patient places restrictions on disclosure of e-results information (see **appendix A section 5.3**)

6. Liasie with local Data Protection & IT Security Officers and/or Caldicott advisor to ensure that:

   a) The procedures for removal of access permissions fits with other NHS Scotland IT security policies and procedures that are in place (see **section 8.9**)
   b) Violation of the terms of the local SCI Store access protocol results in immediate removal of user permissions and that a formal management procedure is in place for such circumstances (see **section 8.9**)
   c) An accurate audit log is maintained of all breaches to the SCI Store Access Protocol at local level, and the audit log is reviewed at regular intervals (see **section 8.9**).
   d) Feedback is provided for formal national reviews of the 'best practice' guidance (see **section 12.3**)

7. Involve Schlumberger/SEMA, HR and IT Trainers from Acute/Primary Care in developing:

   a) Appropriate Local SCI Store Training Material (see **section 8.7**)
   b) Ensuring that SCI Store users are well aware of their statutory responsibilities and Health Board policies and procedures with regard to data protection and maintaining patient confidentiality (see **sections 4, 6, 8.7 & 8.8**)
   c) Arranging regular up-dates in organisation policies and procedures following initial training (see **section 8.7**).

8. Meet with the SCI Store System Administrator and local IT Security Officer to both set-up and agree appropriate audit mechanisms at local level (see **section 11**)

9. Set-up monitoring & review process for the local SCI Store Access Protocol (**section 12**)

10. Seek sign–off approval for local SCI Store Access Protocol from the Health Board Caldicott Guardian and Chair of the ECCI Project Board

Appendix B

1. Guidance for Managing Patient Confidentiality

1.1 Informing Patients – Effectively

Where patients have consented to healthcare, research has consistently shown that they are normally content for information to be disclosed in order to obtain that healthcare (e.g. between members of health care teams and between different organisations). But it is still very important that reasonable efforts are made to ensure that patients understand how their information is to be used to support their healthcare and that they have no objections. For example '*all information about your diagnostic test results is held centrally on a database, but only accessed appropriately on a 'need to know basis'*. Explanations must be proportionate to risks involved and reflect, where possible, the patient's particular circumstances.

In order to inform patients properly staff must:

- Check patients have received appropriate information
- Ensure suitable leaflets are available within the GP Practice/Hospital setting
- Make clear to patients when information is being recorded
- Make clear to patients when information will be disclosed to others e.g. with electronic results *'at your next appointment the practice nurse will be able to view your test results and will advise you appropriately'*
- Check that patients are aware of the choices available in respect of how their information may be used or shared
- Check that patients have no concerns or queries about how their information is used
- Answer any queries personally or direct the patient to others who can answer their questions
- Give information about the right of patients to have access to their e-health records

1.2 Patient Access

Patients have a right to see and/or have copies of their health records under the Data Protection Act. (see **http://www.show.scot.nhs.uk/confidentiality**) It provides guidance on charges, procedures and exceptions. SCI Store Audit logs can also provide details of when, and by whom a patient's sensitive personal data was requested during a specified period. This enables a patient to see who has been looking at their sensitive personal data.

In the not too distant future NHS Scotland patients will be able to electronically access their health care data, check accuracy, amend and/or request up-dating of their data in SCI Store. At present, a facility offered by some GP Practices to patients is secure web browser access to their test results via the GP Practice web site.

1.3 Patient Choice - Consent

Patients have the right to choose whether or not to accept a form of care, whether information about their care can be disclosed to others,and whether or not information that can identify them can be used for non-healthcare purposes. In order to make valid choices patients must be given sufficient information to know what their options are, but also what the consequences are of making certain choices.

Consent can be either implied (when a patient, having been given information about a disclosure, and opportunity to express an objection, accepts a service without voicing an objection) or express consent (when a patient actively expresses consent). Consent whether implied or expressed must always be preceded by effective information and involvement of the patient.

Express consent is 'best practice' and should become the norm as better informed patients share in decisions about the uses of their information. Consent should be obtained at the earliest opportunity.

Where patients have been effectively informed of proposed information sharing and their rights, the NHS will assume it has permission to share any information needed to provide care unless the patient has requested it not be shared.

Requirements for consent should be considered against each of the following criteria:

- Legal requirements
- To protect the patient's vital interests
- In the interest of the public
- Children and adults who are unable to consent (for further information see – **http://www.show.scot.nhs.uk/confidentiality**).

1.4 Patient Refusing or Restricting Disclosure of E-Results Information

Patients can ask that certain parts of their health information be restricted from normal accessing/sharing. Access to e-Results information in SCI Store can be restricted to requesting location, requestee or patient.

In most cases, it will not be possible to restrict e-Results information disclosure without compromising care. In such circumstances patients need to be informed of any possible implications for their own care and the potential effect on others from a decision to withhold their data. This would require careful discussion with the patient, clear explanations on how their data is used, and reassurance around any third party access being only to anonymised data.

NHSScotland patients will be informed that it is not currently technically possible to restrict how their electronic test results are accessed. This is due to the fact that current software developments do not support opting out (use of sealed envelopes and pseudonymisation).

1.5 Procedure for Management of Disclosure Without Consent

In an emergency, if the patient is unable to give consent, doctors must be able to override restrictions and look at information that the patient has restricted (Schedule 3 of the DPA Act 1998). Although this can be done with paper records, the functionality required to do so electronically is not yet available in SCI Store.

Others not treating the patient might in very limited circumstances gain access to the patients e-results in SCI Store records without consent if the law allows it or requires it. (Schedule 2 & 3 DPA Act 1998).

If information is disclosed without consent, then full details must be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. Individual Health Board SCI Store Access protocols must specify the person responsible for ensuring this happens.

Recipients of the information must be made aware that it has been disclosed without consent and must put agreed security procedures in place.

Appendix C

1. Procedures for Protecting Patient Information

1.1 Confidentiality is a contractual obligation for all NHSScotland staff, external contractors and volunteers

i) All NHS Scotland employees must have a statement about the employee's responsibility for confidentiality and information security included in the terms and conditions of their employment.

ii) All NHSScotland employees who have access to Personal data about patients (such as held in SCI Store) must sign a confidentiality statement at the beginning of their employment and good practice is to have confidentiality guidelines reviewed and confidentiality statements re-signed at regular intervals

1.2 NHS Scotland Staff must know their obligations

i) The duty of confidence arises out of the common law of confidence, professional obligations and also staff employment contracts. All NHS Scotland employees, students, external contractors, temporary staff and volunteers are contractually bound by the NHS Scotland Confidentiality NHS Code of Practice on Protecting Patient Confidentiality (see **http://www.show.scot.nhs.uk/confidentiality**). Breaches of confidence, inappropriate use of health records or abuse of computer systems will lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings.

ii) Staff should ensure that they are aware of the requirements and standards of behaviour that applies, and should be trained to deal with them in an appropriate manner.

iii) Professional guidelines require clinicians to ensure that patients are informed about how information about them is used and that consent requirements are met

1.3 Accurate and consistent Information Recording

Maintaining proper records is a vital part of patient care. If records are inaccurate future decisions may be wrong and harm the patient. Information may be needed not only for the immediate treatment of the patient, but the audit of that care and also to support future research. In addition, a requirement of the DPA Act 1998 is that only as much information as is appropriate should be recorded.

1.4 NHSScotland staff must keep patient e-information private – this includes:

- Ensuring discretion in discussions with clinical colleagues
- Taking care when discussing cases in public
- Not seeking to access information on individuals whose treatment they are not involved in

With electronic lab results staff must:

- Always log-out of the computer system application when work on it is finished
- Not leave a terminal unattended and logged-in
- Not share logins with other people
- Not reveal passwords to others or write them down
- Change passwords at regular intervals to prevent anyone using them
- Avoid using short password or using names or words that are known to be associated with the user or system
- Passwords must comprise minimum 6 characters, at least one of which should be a non-alphabetic character
- Not reuse a password they have used in the past
- Ensure that when entering their password, the entry cannot be seen by anyone else
- Always clear the screen of a previous patients information before seeing another.
- Use a password protected screen-saver to prevent casual viewing of patient information by others

Appendix D

Ayrshire & Arran Acute Hospitals NHS Trust

Please return to:
Leigh McPartland
ECCI User Support Officer
14 Lister Street
Crosshouse
KA2 0BE

I M & T Department

System Access Request Form

Requested System to access ...electronic Lab Results Reporting

USER INFORMATION

Please complete one of these boxes if you already have a username

dr	nu	ms	cr	Other

I agree to abide by the Trust's published rules & Codes of Connection with respect to the above System

Surname (PRINT)		Forename (PRINT)		Job Title	
Base		Dept		Ext	
Signature				Date	

Manager Confirmation (this section is not required for Medical Staff)

I confirm the above member of my staff has a business need to access to the requested system and that I will be responsible for any incremental charges incurred by providing this access. I will inform IM&T if the situation changes.

Name (PRINT)		Title	
Dept		Ext	
Signature		Date	

System Owner confirmation (names available from the IM&T Help Desk)

I confirm that giving the above access is consistent with Trust Policy

Signed		Title	
Level of access		Date	

IM&T Use

Initials	Date	ID Allocated
Initials	Date	Receipt returned

Appendix E



1. Pathology Test Results Electronic Reporting

Laboratory Name :
Laboratory Address :
:
:
:
Phone Number :

GP Practice Name :
GP Practice Address :
:
:
Phone Number :

2. Partnership Agreement

Synopsis: The Partnership Agreement lays out the areas of agreement on relevant issues relating to the exchange of data by electronic interchange between participating partners. The agreement reflects decisions taken by both sender and recipient before electronic communication takes place.

Date: 13 August 2003

Author: Richard McEwan
ECCI Project Manager

1. Parties Involved

This agreement relates to the exchange of clinical electronic messages between the following parties.

2.1 NHS Trust

Trust Department	Pathology
Hospital	
Trust Name	
Address	

2.2 GP Practice

GP Practice Name	
Address	

2.3 Contacts

The Following persons will act as main points of contact over any user related issues in connection with the exchange of electronic Pathology Test Reports.

2.3.1 Trust Contacts

Title	Contact	Contact Details
Pathology Laboratory Systems Manager		Tel: Email:
Pathology Laboratory Manager		Tel: Email:

2.3.2 GP Practice Contacts

Title	Contact	Contact Details
Practice Computer Manager		Tel: Email:
Practice Manager		Tel: Email:

2.3.3 GPASS Contacts

Title	Contact	Contact Details
Helpdesk		Tel: 0141 882 9998 Email:

2.3.4 ECCI/SCI Contacts

Title	Contact	Contact Details
ECCI/SCI Project Manager	Richard McEwan	Tel: 01698 855592 Email: Richard.McEwan@lanpct.scot.nhs.uk

2. Information To Be Exchanged

2.3.5 Laboratory Reports

Specialties

Results we transmitted to the SCI Store and made available for importation into GP systems for the following Pathology specialties:

- Clinical Chemistry
- Haematology
- Microbiology
- Immunology

2.3.6 Frequency And Timing Of Results Dispatch

Results will be transmitted every 20 minutes to the SCI Store. Results will be collected from the SCI Store by the GP system between 7 and 9 am daily.

2.3.7 Urgent Reports

Reports considered to be of Clinical significance will be communicated by telephone.

2.3.8 Hard Copy Reports

Hard copy reports will continue to be sent to the Practice in the usual manner until both parties agree on their cessation.

3. Error Situations

Problems with results or patient demographics: contact the appropriate Laboratory concerned.

Problems with IT equipment or networks: Contact appropriate IT Help Desk.

Problems with SCI Store: Contact ECCI/SCI Project Manager.

Problems with GP Upload Software: Contact GPASS Helpdesk.

4. Responsibilities

2.3.9 Trust Responsibilities

- Successful delivery of all reports to SCI Store.
- Inform ECCI/SCI Project Team of any changes or additions to Laboratory tests or mnemonics.

2.3.10
2.3.11 GP Practice Responsibilities

- Provision of accurate patient information on request forms and specimens. All request forms should contain the patients CHI number, preferably using barcoded labels. Results for requests with no CHI number will not be made available for upload into GP systems but will be available for viewing on SCI Store.
- Provision of accurate requester and Practice information on request forms.
- Inform the appropriate Laboratory if results have not been received for a particular request or if results are received for patients who do not belong to the Practice.

2.3.12 ECCI/SCI Responsibilities

- Maintain all mapping tables for tests, GP's and Practices.
- Maintain interfaces with all systems.
- Maintain bounded READ code mapping tables.

2.3.13 GPASS Responsibilities

- Installation and maintenance of GP upload software.
- Maintenance of GPASS – SCI interface.

2.3.14 All

- All parties will be responsible for the installation of the latest software releases and hardware implementation as required.
- All parties will be responsible for respective training.
- All parties will be responsible for ensuring that obligations under the Data Protection and Caldicott Guidelines are observed.

5. Agreement

2.3.15 For: [Laboratory Name Here]

Name:

Post within organisation:

Date:

2.3.16 For: [GP Practice Name Here]

Name:

Post within organisation:

Date:

Appendix F

Acknowledgments

First of all our thanks go to all those that contributed to the wider consultation exercise at the Stirling Royal Infirmary Management Centre on the 2nd September 2003. Many of the responses to this consultation exercise were challenging and helpful. The recommendations in this guidance address these and many other issues.

As a fall-out of the wider consultation exercise the SEHD e-Results Best Practice Guardians Sub-Group was formed. The expertise and experience of the members of this group contributed much to the development of this document. We have also valued the views of SEHD Caldicott Advisor, SEHD IM&T Strategist, Lothian and Lanarkshire Laboratory Services Medical Directors and the Consumer Council for Scotland.

The SEHD e-Results Best Practice Guardians Sub-Group consisted of a chair, Ms. Kirsty MacLeod, SEHD ECCI Facilitator and 8 members from a variety of professional backgrounds:

Dr. Kennneth Robertson	SEHD Clinical Lead Health Informatics
Ms. Anne Lamont	ISD SCI Programme Manager
Dr. Paul Cawood	Clinical Scientist/Biochemist Lothian HB
Dr. Frank Finlay	Clinical Scientist/Biochemist Greater Glasgow HB
Mrs Denise Brown	ECCI Project Manager Ayrshire & Arran
Ms. Tracy McKinnley	Information Manager West Lothian Trust
Mr Campbell MacLean	Schlumberger/SEMA Project Manager
Mr Shawn Doney	Schlumberger/SEMA Technical Advisor

Glossary of Definitions

Clinician in respect of diagnostic laboratory tests, a **'Clinician'** is a health care professional responsible for delivering advice or treatment to a patient based on the results of their laboratory investigations, e.g. doctors, nurses, laboratory scientist, physiotherapist, dieticians and pharmacists.

Need to Know is interpreted as meaning that members of an organisation should have access to information if the function or role which they are charged with fulfilling at that particular point in time in relation to a particular person, cannot be achieved without access to the information specified

Privacy the right of an individual to retain personal information to themselves (which may include the right to suppress information already held by others)

Confidentiality the duty to keep secret privileged information received concerning others to prevent loss, damage or embarrassment to those concerned (with the potential to be sued for any breech)

Security the need to keep information accurate and available only to those properly authorised (so includes preventing loss, corruption, or access by those not properly authorised – it also includes ensuring that the data is available to those who should have it)

3rd Party Persons other than:
- the data subject
- the data controller
- employees/agents of the data controller/processor

Data Controller Person(s) who determines the purpose for which and manner in which any Personal data (or are to be) processed

Appendix G

REFERENCES

NHS Scotland Code of Practice on Protecting Confidentiality (NHSScotland July 2003)
http://www.show.scot.nhs.uk/confidentiality

Department of Health confidentiality Code of Practice (DOH July 2003)
http://www.doh.gov.uk/ipu/confiden

NHS Information Authority 'Caring for Information – Model for the Future' (NHSIA October 2002) http://www.nhsia.nhs.uk/confidentiality

Share with Care – NHSIA & Consumers Association 'Peoples views on Consent and Confidentiality of Patient Information' (October 2002)
http://www.nhsia.nhs.uk/

Gaining Patient Consent to Disclosure Cambridge Health Informatics: A Consultancy Project for the NHS Executive January 2001 (Department of health publications
http://www.doh.gov.uk

Relevant Web sites

http://www.show.scot.nhs.uk/dataprotection

http://www.show.scot.nhs.uk/security

Electronic Privacy Information Centre http://www.epic.org

Privacy International http://www.privacyinternational.com

Home Office http://www.homeoffice.gov.uk

Foundation for Information Policy Research http://www.fipr.org.uk

NHSIA Security & Data Protection Programme http://www.standards.nhsia.nhs.uk

Info. Security of Telecommunications and Information systems
http://www.cordis.lu/telematics/home.html

APPENDIX H: Example of SCI Store – General Practice E-Results Access Matrix

	User Types										
Document Types	General Practice Doctors	Locum Doctor 1*	Locum Doctor 2*	Practice Nurse	District Nurse	Health Visitor	Midwife	Community Staff Nurse	Practice Manager	Practice Admin Staff	Pharmacist
Patient Demographics	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1	NC2	C1
Haematology Result Reports	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1	NC2	C1
Biochemistry Result Reports	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1	NC2	C1
Microbiology Result Reports	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1	NC2	C1
Pathology Result Reports	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1		C1
Immunology Result Reports	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1		C1
Virology Result Reports	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1		C1
Radiology Summary Reports	C2	C2	C2	CN3	CN3	CN3	CM4	CN3	NC1		C1

* Locum 1 Primary Care Trust Contracted *Locum 2 Itinerant Locums

Role Based Access Levels:

Community Clinician Level 1 – All Results in SCI Store (excluding restricted access areas) (C1)
Community Clinician Level 2 – All GP Practice Patients Results only (excluding restricted access areas) (C2)
Community Clinician - Nurse - Level 3 – All GP Practice Patients Results only (excluding restricted access areas) (CN3)
Community Clinician – Midwife – Level 4 - All Results Women (> 9 yrs <50 yrs & babies < 1 yr) (CM4)
Community Non-Clinician Level 1 – All GP Practice Test Results in SCI Store (excluding restricted access areas) (NC1)
Community Non-Clinician Level 2 – Access to certain GP Practice Results only (NC2)