Access Protocol for

The Emergency Care Summary

System

Version 5.0
10th July 2013

NB: any paper version is only valid on the day of printing

DOCUMENT CONTROL SHEET

Title:	***Access Protocol for the Emergency Care Summary***
Date Published/Issued:	*10 July 2013*
Date Effective From:	
Version/Issue Number:	*5.0*
Document Type:	*Access protocol for ECS*
Document status:	*Draft*
Author:	*Jonathan Cameron, Libby Morris and Ernest Beattie*
Owner:	*Chair of ECS Service Management Board – Dr Ian Thompson*
Approver:	*Dr Ian Thompson, Chair of ECS Service Management Board,* *Dr Lorna Ramsay, Medical Director NSS IT*
Approved by and Date:	*ECS Service Management Board 10th July 2013*
Contact:	*Ernest Beattie, NISG*
File Name:	*ECS website*

Revision History:

Version	Date	Summary of change	Owner
3.0	11/11/2011	Revision to new template and references updated by K. Kingan	Jonathan Cameron / Libby Morris
3.1	18/04/2012	Updated by Ernest Beattie to reflect various changes and expand linked documentation section	Ian Thompson
4.0	15/02/2013	Updated to reflect extension of access to scheduled care	Ian Thompson
5.0	09/07/2013	Updated to incorporate additions requested by the ECS Service Management Board	Ian Thompson

Approvals: This document was formally signed off by:

Name:	Signature:	Title:	Date:	Version:
Ian Thompson		*Chair ECS Service Management Board*		
Dr Lorna Ramsay		*Medical Director, NSS ITSBU*		

This guidance is available on the website *(insert link)* and was formally issued under…….

Distribution: This document has been distributed to

Name:	Title/Division:	Date of Issue:	Version:
ECS Service Management Board		10th July	5.0
Caldicott Guardians			5.0
IG Leads			5.0
ECS Audit Group			5.0

Linked Documentation:

Document Title:	Document File Path:
NHS Scotland ECS Governance Protocol for NHS Board Unscheduled Care Service Cross Boundary Access to Patient ECS Records	Central location to be determined.
eHealth Strategy 2011-17	http://www.scotland.gov.uk/ehealthstrategy2011-2017
Clarification of access to Emergency Care Summary – CMO (2008) 05	http://www.sehd.scot.nhs.uk/cmo/CMO(2008)05.pdf
Extension of ECS Access to Scheduled Care Settings in Support of Medicines Reconciliation	http://www.sehd.scot.nhs.uk/cmo/CMO(2011)16.pdf
CEL 45 (2008) - Scotland Mobile Data Protection Standard	http://www.ehealth.scot.nhs.uk/wp-content/documents/cel-452008-common-encryption-standards.pdf
NHSScotland Standards re User Names & Passwords	http://www.ehealthrepository.scot.nhs.uk//wp-content/documents/architecturedesign/Standard%20-%20Password%20Standard.doc
ECS Audit Reporting User Manual	http://www.ecs.scot.nhs.uk/wp-content/uploads/ECS-Audit-Reporting-User-Manual-V4.0.pdf
Protecting Patient Confidentiality, Final Report, CSAGs, 2002	http://www.sehd.scot.nhs.uk/publications/ppcr/ppcr.pdf
Confidentiality: NHSS Code of Practice, 2003	http://www.ehealth.scot.nhs.uk/wp-content/documents/nhs-code-of-practice-on-protecting-patient-confidentiality.pdf
NHSScotland Information Security Policy, (HDL(2006)41)	http://www.sehd.scot.nhs.uk/mels/hdl2006_41.pdf
Caldicott Guardian Manual, 2010, (Scottish version)	http://www.scotland.gov.uk/Resource/Doc/340362/0112733.pdf
Records Management: NHS Code of Practice (Scotland) V2, 2010	http://www.scotland.gov.uk/Publications/2010/04/20142935/0
Information Commissioner's Office Guidance	http://www.ico.gov.uk/for_organisations/guidance_index.aspx
IT Security Policy	http://www.security.scot.nhs.uk/?page_id=61
Computer Misuse Act 1990	http://www.legislation.gov.uk/ukpga/1990/18/contents
Data Protection Act 1998	http://www.legislation.gov.uk/ukpga/1998/29/contents
ICO Privacy Notices Code of Practice	http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_notices.aspx
National ECS Leaflet	http://www.scotland.gov.uk/Publications/2006/08/16152132/2

Human Fertilisation & Embryology Act	http://www.legislation.gov.uk/ukpga/2008/22/contents
NHS Venereal Diseases Regulations 1974	http://www.legislation.gov.uk/uksi/1974/29/contents/made
Abortion Regulations 1991	http://www.legislation.gov.uk/uksi/1991/499/contents/made
Gender Recognition Act 2004	http://www.legislation.gov.uk/ukpga/2004/7/contents
Records Management: NHS Code of Practice (Scotland) Version 2 (2010)	http://www.scotland.gov.uk/Publications/2010/04/20142935/0
BIP 0002:2003 Guidelines for the use of personal data in system testing :	http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030100005

INDEX

1. OVERVIEW

1.1 Purpose

This protocol sets out the information governance and access arrangements for the Emergency Care Summary system. The aim is to ensure effective use of the system, in accordance with legal/professional requirements and best practice. This document is an updated version of the Audit and Access Protocols for ECS which were published in 2006 as part of the national rollout of the system.

1.2 Policy and strategy context

NHSScotland aims to provide safe and effective care, and availability of information is crucial to that aim. There is a need to ensure that appropriate information is available when it is needed, accessed only by those who should have access to it, and that it is correct and up to date.

ECS is considered a critical system to support the aims of the eHealth Strategy and Quality Strategy for NHSS.

1.3 Objectives

The objectives of this policy / protocol are to ensure that there is clarity around:

- Authentication: the identity of the individual users
- Authorisation: what the individual users are permitted to do
- Assurance: what actions individuals have undertaken
- Agreement: the level of consent required / relied on for these actions.

Specifically, the protocol will:

- Provides a robust information governance (IG) framework for the legal and ethical obligations that underpin the management of access to information held on the Emergency Care Summary by authorised users for a defined purpose(s)
- Describes the mechanism for extraction of the data from the Primary Care system to ECS store and the process for managing amendments to ECS data in the store.
- Describes the structures that must be in place to safeguard patient information
- Reference the authorisation rules for granting access to ECS information in ECS store.
- Defines the security, access permissions for access to data in the ECS store, Role based access, registration, user account management and authentication processes, and training requirements.
- Defines ECS operational issues, roles & responsibilities
- Describes the processes that must be in place to inform patients how their ECS information will be held, how it is used and shared in line with statutory responsibilities and patient choice.
- References the audit procedures that must be undertaken
- Sets out how this framework will be implemented, monitored and reviewed.

1.4 General principles

In operating and using the system the Caldicott principles shall apply, i.e.

- Justify the purpose(s) of using confidential information
- Do not use patient-identifiable information unless it is absolutely necessary

- Use the minimum necessary patient-identifiable information that is required
- Access to patient-identifiable information should be on a strict need-to-know basis
- Everyone with access to patient-identifiable information should be aware of their responsibilities
- Understand and comply with the law

2. SYSTEM BACKGROUND/CONTEXT

Background

The previous guidance was published in September 2006 (Ref: NHS Scotland ECS Governance Protocol for NHS Board Unscheduled Care Service Cross Boundary Access to Patient ECS Records[1]) and in light of the extension to the scope and the user base of ECS, a further review and update of the Access Protocol has been undertaken. This protocol has also been updated in the new standard eHealth template.

2.1 Why the Emergency Care Summary is needed and what are its benefits

The Emergency Care Summary is an important component in delivering the eHealth Strategy[2] and also the quality strategy which states that care will be safe, effective, efficient, equal, patient centred and timely.

The ECS provides access to key patient information out of hours to support any form of unscheduled care and from 2012 will include full information on patients needs and wishes in order to support anticipatory care plans for all patients who need it.

Following the publication of the letter from the CMO in December 2011 Extension of Emergency Care Summary Access to Scheduled Care Settings in Support of Medicines Reconciliation CMO(2011)16, the ECS now provides access to support schedule care.

Benefits

Patients benefit from having crucial medical details available for clinicians who are caring for them This can lead to safer care, e.g. having a list of prescribed medications available for patients who are ill or confused, and will support medicines reconciliation

Clinicians benefit from having medical information on patients which can influence prescribing decisions and increase confidence for decision making

2.2 What does it do?

The ECS store is the clinical data repository used by all NHS boards to hold Emergency Care Summary records.

ECS records are composed of core demographic data, prescribing and adverse reactions to medications if recorded in the Primary Care electronic system records. An initial download of data is transferred when a practice connects to the ECS store, and thereafter any changes to the items in the Primary Care system will automatically be

[1] NHS Scotland ECS Governance Protocol for NHS Board Unscheduled Care Service Cross Boundary Access to Patient ECS Records
[2] eHealth Strategy 2011-17

updated twice daily to the database hosted on a server within the Atos Data Centre in Livingston.

The ECS records are available on a “read only” basis to clinicians caring for patients in Emergency and Unscheduled Care, including OOHs, NHS24 and A&E departments. Clinicians in scheduled and continuing care with a legitimate role in the care of a specific patient and also relating to medicines reconciliation can also view that patient’s ECS record. The CMO Guidance on ECS use published in August 2008 and December 2011 sets out who is entitled to access ECS.

The electronic Palliative Care Summary (ePCS) has been implemented as an extension to the ECS core data set and.a further extension, the Key Information Summary (KIS) has been developed and is currently being rolled out across all boards

Future enhancements may include the addition of vaccination information.

2.3 Where is it in operation?

In line with CMO Guidance[3][4] on ECS, the following user groups are approved to use ECS:

Unscheduled Care
- NHS24
- Out of Hours (OOH)
- A+E Departments
    - Including Pharmacists
- Acute Receiving Units
- Medical receiving Units
- Scottish Ambulance Service (SAS)

Scheduled and Continuing Care
- Outpatient Appointments
- Arranged admission
- Periodic review of patients with long term conditions

Hospices have also been approved for access to ECS as part of the ePCS rollout.

ECS is used in 17 boards across NHSS:

- All 14 Territorial boards
- NHS24
- Scottish Ambulance Service
- National Waiting Times Centre (Golden Jubilee National Hospital)

NHS National Service Scotland (NSS) members of staff do not have access to patient information on ECS but do have access to Management and Performance information.

---

3 CLARIFICATION OF ACCESS TO EMERGENCY CARE SUMMARY – CMO (2008) 05

4 EXTENSION OF ECS ACCESS TO SCHEDULED CARE SETTINGS – CMO (2011) 16

Access by health care staff working in prisons was approved by the ECS Programme Board in May 2011, as part of the transfer of prisoner healthcare to the NHS in November 2011.

3. SYSTEM USERS AND ACCESS CONTROLS

Access controls are only part of wider managerial policies and procedures, which in combination with robust IT security practices and standards serve to protect confidentiality. A fundamental safeguard is confidentiality being a professional and/or contractual obligation on all NHSScotland staff, and staff knowing their obligations

In line with this, confidentiality is addressed for the system through a wide system of information governance measures. These are covered in more detail in the sections below.

3.1 Who uses the system, what do they use and for what purpose?

Access permissions are restricted to the following uses:

- Direct patient care
- Security audit
- Management information
- System maintenance
- Patient requests
- Medicines Reconciliation

a) Health care professionals working in unscheduled care organisations, OOHs, NHS24, A&E and Acute receiving units with responsibility for delivering advice or treatment to a patient. This includes doctors, nurses and pharmacists who have a legitimate clinical relationship with the patient and who have either been given appropriate consent or have taken a clinical decision to access without consent 'break glass' as defined later in this document.

b) Admin staff in all of these locations can use the demographic records when carrying out admin and audit functions.

c) Clinicians in scheduled care with a legitimate role in the care of a specific patient and with a role relating to medicines reconciliation in order to check the accuracy of GP prescriptions for that patient.

d) Admin staff in GP Practices can access audit logs as a security measure to verify whose notes have been accessed. This access is restricted to patients registered with their own practice.

e) Patients can ask their GP practice to print a copy of their own ECS record if they wish.

f) Systems Administrators require to access the system to ensure user accounts are kept up to date (on instruction from a clinical authority) change passwords and to monitor access.

g) Authorised technical support staff to diagnose and correct faults and ensure the system works effectively.

h) Access to Management Information is available to NSS staff to report on use and issues on ECS.

Information on the ECS store must only be accessed on a genuine 'need to know' basis. This means that those who access a patient's information must

- Be who they claim to be through identity checks,
- Are authorised users of the system
- Have a legitimate care relationship with the patient
- Only see information their role allows

Data is not permitted to be used for any secondary uses, clinical audits or research. Statistics are used for reporting purposes but do not include any identifiable patient information or clinical details. Accesses are recorded and audited and statistics for local and national returns prepared on a continuous basis.

Mobile devices are used by OOHs clinicians via the ADASTRA Aremote system and by SAS using in-cab terminals for paramedics. These arrangements comply with the NHS Scotland Mobile Data Protection Standard[5].

An audit trail is kept of all users actions, from search criteria through to the patient's record which is viewed or rejected. Need to know cannot be enforced through IT system security alone, but in combination with managerial policies and procedures. Access will be controlled on a defined user role based access and the individual must follow IT security and confidentiality procedures and be prepared to justify any challenges on appropriateness of access.

The privacy breach detection solution, FairWarning, is being implemented in all territorial Boards and those special Boards holding patient identifiable data to strengthen existing surveillance and detection capabilities within electronic health information systems including ECS.

3.2 Registration and management of user accounts

Registration of users

Users of the ECS web browser must be formally registered by the ECS store administrator. A standard user registration form is located at appendix A and procedures must ensure that identification and verification of the users is compatible with their entitlement to access The ECS system administrator must only create new user accounts on receipt of fully completed request forms, and all user registration details must be reviewed at least every six months in conjunction with the relevant line managers to ensure that access is still authorised.

Role based access privileges

The access given to all authorised users is to the complete dataset. Whilst access is not role specific, usernames and passwords are unique, there are no generic usernames.

Management of user accounts

[5] CEL 45 (2008) – NHS Scotland Mobile Data Protection Standard

Maintenance of user accounts is the joint responsibility of the individual user, the clinical line manager and the ECS store administrator.

The method employed to manage ECS Store User Accounts is a local decision, but it must clearly define roles and responsibilities.

Examples of effective user account management processes are described below:

1) Where access to the ECS Store is via the Standalone web browser utility the local ECS Store System Administrator should run a SQL query in the ECS Store to identify which users have not accessed the facility in the past 3 months and remove/delete their access permissions following appropriate liaison with departments (e.g. A&E).

2) Where access to the ECS Store is via the Out of Hours frontline call management system, the Out of Hours system administrator should run a similar query to identify users who have not accessed the ECS facility in the past 3 months. The report should be brought to the attention of the local Out of Hours Service Manager for consideration of removal/deletion of their access permissions.

3) If at the point of registration of the user it is known that it will be for a specific time then the option of entering at end date is available.

Authorising & Managing Non-Clinical Staff Access to ECS Store

Access can only be provided on the authority of the local NHS Board or Special Health Board ECS Store Data Controller who may devolve the authority to grant access to the appropriate employee's line manager or head of services. Access to ECS Store data for this group will be granted strictly on a need to know basis.

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

- OOH, NHS 24, and A&E department administrative staff who have the initial contact with the patient – able to print out patient ECS record
- The ECS 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 who diagnose and correct faults and ensure the system works effectively.

It is the responsibility of the individual Health Boards to ensure that the correct users are set up and removed when they are no longer authorised for example if they leave the organisation. Atos manages the administrator accounts.

The Special Health Boards, NHS24 and the Scottish Ambulance Service are required to implement similar user authentication

Authentication of users log-on

User access to the ECS Store is controlled by a 'unique user name and password' system that meets the minimum NHSScotland Standard (see http://www.show.scot.nhs.uk/security). This can be either through the user's front-line application or an individual account on the Store. Passwords are time limited, a renewal

period is recommended at 60 days. It is for local management to ensure that user IDs are used by one and only one individual.

3.3 Audit of system use

The provision of an Audit Trail is a fundamental requirement of information governance. Audit Trails enable users to be made accountable for their actions in the system, and offer a security record for use in analysing breaches of security and policy.

Within the ECS Store all 'actions' conducted e.g. search criteria entered, ECS data returned, viewed and/or rejected, are recorded in an audit trail. These in-built audit logs allow identification of all system users who have accessed a patient record over a given period (who, what, where and when). Where a user has direct access to the ECS Store through their local frontline service application e.g. Out of Hours system Adastra, the frontline application system (as well as the national ECS Store) will maintain an audit trail of all ECS search queries, and record accesses.

To ensure compliance with the local Access Protocols, audits must be undertaken on a regular basis by suitably authorised personnel within each NHS Board (i.e. ECS Store system administrator and user support staff). NHS organisations must be in a position to demonstrate their ECS Store audit procedures on request by their NHS Board.

Good practice for audits includes regularly looking for atypical usage e.g.:

- Repeated unsuccessful access attempts
- Wrongly submitting password 3 times
- Long periods worked by an individual user
- Casual browsing

The implementation of the FairWarning privacy breach detection tool will provide Boards with a number of reports which will assist in carrying out the audits.

Each request to the ECS Store is audited with the following information:

- Date & time of event
- The client role (e.g. OOH)
- The client NHS Board
- The recorded username of the client system
- The registered Health Board name of the user
- The client system, IP address
- The request type (demographic, clinical or ePCS)
- The context of the request (e.g. if a search has been requested then the context will hold the search criteria entered)

An ECS Audit Reporting User Manual[6] has been produced for the use of the ECS Auditors detailing the reports produced and the actions to be carried out.

3.4 Contractual obligations

NHSS staff are contractually required to comply with standards, Codes of Practice and good practice in relation to confidentiality and security of information e.g.

- Professional standards of conduct
- Relevant Scottish Government publications such as

[6] http://www.ecs.scot.nhs.uk/wp-content/uploads/ECS-Audit-Reporting-User-Manual-V4.0.pdf

    - Protecting Patient Confidentiality, Final Report, CSAGs, 2002
    - Confidentiality: NHSS Code of Practice, 2003
    - NHSScotland Information Security Policy, (HDL(2006)41)
    - Caldicott Guardian Manual, 2010, (Scottish version)
    - Records Management: NHS Code of Practice (Scotland) V2, 2010
- Information Commissioners Office
- Good practice Notes
- Codes of Practice
- Technical Guidance Notes

3.5 Data Protection Act

Privacy Impact Assessment (PIA) outcome

Although the PIA process was not in place when the initial ECS was created, PIAs have subsequently been completed for ePCS and KIS. Copies of these PIAs are attached in Appendix A.

Table 1 confirms that ECS meets the public / patient information requirements in line with the Data Protection Act.

Table 1: DPA - public / patient information requirements

Information requirement	**Covered in line with Data Protection Act?**
Who is the data controller	See paragraph below
Description of the personal data held	Yes
Purposes for which the data are to be used	Yes
Who the data are disclosed to	Yes
Where they have the right to do so, their right to opt out but with consequences made clear to them	Yes
Their access rights	Yes

Data Controllers

The data controller is the organisation that determines how and for what purposes, patient identifiable information is collected, held and processed.

In relation to the national ECS Store the responsibilities are as follows:

1. NHS Scotland General Practitioners are the Data Controllers in respect of the clinical and demographic patient information they submit to the National ECS Store up to the time of submission.

2. NHS Boards are responsible for the safe delivery of health care to their patients wherever they present for health care within NHS Scotland, and are Data Controllers in respect of the information about patients that they hold in the National ECS Store. At NHS Board level the individual with overall responsibility for Personal Health Information is the Chief Executive. He or she may delegate this responsibility to their Director of Public Health/Medical Director/Caldicott Guardian. In turn the DPH/MD/CG may delegate this responsibility to the appropriate heads of department.

3. The Common Services Agency, now known as National Services Scotland, (NSS) are the Data Processors for the data within the ECS Store, and responsible for the day to day operational management of the national utility. NSS performs these two roles under instruction from the Scottish Government Health & Social Care Directorate.

3.6 Awareness & training

All users must be briefed on:

- Local User Training and Awareness materials
- The fact that "live patient details" **MUST NOT** be used for training purposes
- IT Security Policy
- The Computer Misuse Act, 1990
- The Data Protection Act, 1998
- NHS Scotland Code of Practice on Protecting Confidentiality

All users must be made aware of their responsibilities regarding confidentiality and security before access to ECS Store is given. Training must be provided and should include guidance on what may constitute inappropriate access. In addition, all IT users must be reminded that there will be an audit trail to identify any breaches of confidentiality; that action will be taken where breaches are identified; and that such action might include disciplinary action (including reporting to professional bodies).

Initial training must be followed-up by regular up-dates of organisational policies and procedures.

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

All users must be reminded (verbally and in writing) of their legal and ethical responsibilities in respect of data protection.

3.7 Monitoring and holding to account

Will be at different levels

- NSS - via specified returns in accordance with agreed timescales
- NHS Boards - via high level IG reports in accordance with agreed timescales
- NHS Board Clinical Governance Committee - via system specific IG reports in accordance with agreed timescales

Management of confidentiality and security

- At NHS Health Board level, responsibility for the system resides with (name & title)[7] who will ensure that the Board is kept informed of any relevant confidentiality and security issues.
- Responsibility for implementing, monitoring, documenting and communication confidentiality and security issues for the system resides with (name & title)
- The custodian of the IT assets associated with the system is (name & title)
- Responsibility for continuity and disaster recovery of the systems resides with (name & title)

[7] NB: This person is expected to be an Executive Director as described in the national standards

- Responsibility for auditing the policy / protocol for the system resides with (name & title).

3.8 Dealing with a (suspected / potential) breach

The following types of incidents must be logged to the organisation's Information Governance Lead or Information Security Officer and the appropriate incident form completed:

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

4. SPECIFIC ROLES AND RESPONSIBILITIES

The ECS Service Board has overall responsibility for putting in place and maintaining up to date IG arrangements. This includes ensuring that all key roles & responsibilities for the ECS are clear and are operational.

Table 2 (overleaf) summarises the current position.

Table 2: IG roles & responsibilities

Role / Responsible organisation(s)	NSS	ECS Service Board	NHS Boards	GP Practices	3rd parties, *e.g. commercial contractors*	Users e.g. NHS24, SAS
Data controller(s)[8]			Joint	In common		
Data controller(s) of any linked national system[9]			X	EMIS, Vision		
System Administrator	X		X		X - AOA	
Data processors	X				X - AOA	
Awareness and training • development • delivery			X Development and Delivery	X Delivery		X Development and Delivery
Quality assurance of data input				X		
Integrity of the database					X - AOA	
Ongoing access security management			X			X
Monitoring adherence to the protocol	X	X	X			X

[8] *Where there are multiple data controllers, specify whether these are "joint" (using the same data for the same purpose) or "in common" (using the data for different purposes)*

[9] They need to be involved to ensure clarity about who needs to do what when national IT systems are required to exchange data

Audit	X	X	X	X		X
Dealing with (suspected) breaches, *e.g.* ○ *Who is responsible for informing the ICO if applicable?* ○ *Whether/ how / by whom are patients notified in the event of a breach*			X X	X		
Dealing with disciplinary matters arising from breach investigations			X	X	X	X
Dealing with Disclosures of Information: • Subject Access • FOISA • Police • Research & Development • Service audit	X		X	X		
Dealing with statutory limitations on disclosure of information	X		X			

5. DATA SUBJECT

Arrangements for informing patients & public about the ECS[10]

The following methods are used to inform patients & public about the ECS.

- posters and leaflets in GP surgeries, Out of Hours waiting rooms and A&E departments
- Practices may choose to inform patients via practice newsletters and messages on the RHS of prescriptions.
- NHS 24website.
- Health Rights Information Scotland HRIS (HRIS) website
- Local methods may be used in different Health Board areas appropriate to local circumstances
- More detailed plans and communication materials are available for ePCS and KIS and all materials are available to practices on the ECS website.
- All patients are asked for their consent before any access to their ECS record.

These methods conform to good practice regarding equality and diversity and the information is available in a number of formats and different languages and facilitated by HRIS who are part of Consumer Focus Scotland. .

It is jointly the responsibility of NHS Scotland's GPs to help ensure that patients are informed about the provision of unscheduled care in their area and the existence of ECS. They may wish to inform patients that in order to provide out of hours care safely basic information about them (i.e. medication and allergies) will be made available via ECS to the NHS Board which will be providing their out of hours care.

In order to assist NHS Scotland's GPs a national ECS Leaflet mail-drop to all 2.5 million households in Scotland was conducted at the end of August 2006, along with a telephone help line for enquiries.

The national ECS leaflet has been made available in other formats e.g. audio, Braille, large print, sign language, and in the following community languages; Arabic, Hindi, Chinese, Bengali, Punjabi, Gaelic, and Urdu. Copies of the National ECS Leaflet [11] can be downloaded from the Scottish Government publications web site.

5.1 Need to Know

The Data Protection Act requires organisations to use the minimum amount of personal information on a "need to know" basis.

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

---

10 http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx

11 http://www.scotland.gov.uk/Publications/2006/08/16152132/2

In operating and using the Emergency Care Summary the following principles applies

- Information is only accessed by the people described in this document
- Information is only accessed for the purposes described in this document
- Access is on a "need to know" basis
- Only aggregated numbers of records accessed are used for purposes other than direct care and management
- No secondary usage or research activities are permitted on ECS
- The ECS is not to be used for Clinical Audit

5.1.2 Personal Identifiable Data

In addition to demographic data, ECS holds personal identifiable data relating to allergies and medication.

NHSScotland classifies this data as "sensitive personal data" and requires staff to be especially vigilant when dealing with it.

5.1.3 Sharing of Information

Sharing information about individuals is important for efficient care and improving safety as they move between primary and secondary care.
It is essential that healthcare professionals are able to communicate and share information in order to provide the best possible care for patients.

Patients expect their personal information to be shared between NHS organisations providing them with services. However, they also expect that sharing is safe, secure and only the information that is relevant is shared.

Every organisation must ensure that DPA 'fair processing' obligations are met. This means that each organisation must provide individuals with sufficient information to make them aware of:

Requirement	**Covered in line with Data protection Act?** [If not, insert explanation and planned action]
Who is the data controller	Yes
Description of the personal data held	Yes • CHI Number • Forename, Surname, Previous Surname • Address & Post Code • Date of Birth • Gender
Purposes for which the data are to be used	Yes • Direct patient care • Security audit • Management information • System maintenance • Patient requests
To whom are the data are disclosed	Yes • Health care professionals working in unscheduled care organisations, OOHs, NHS24, SAS, A&E and Acute

	receiving units with responsibility for delivering advice or treatment to a patient and who have appropriate consent • Admin staff in all of these locations can use the demographic records when carrying out admin and audit functions. • Clinicians in scheduled care with a legitimate role in the care of a specific patient and with a role relating to medicines reconciliation in order to check the accuracy of GP prescriptions for that patient. • Admin staff in GP Practices can access audit logs as a security measure to verify whose notes have been accessed. This access is restricted to patients registered with their own practice. • Patients can ask their practice to print a copy of their own ECS record if they wish. • Systems Administrators require to access the system to ensure user accounts are kept up to date (on instruction from a clinical authority) change passwords and to monitor access. • Authorised technical support staff diagnose and correct faults and ensure the system works effectively
Where data subjects have the right to opt out, but with consequences made clear to them	Yes A patient should be given the choice to 'opt out' of having their Emergency Care Summary information on the ECS Store. It is not possible to exclude some items from the ECS Dataset and not others, so if a patient wishes to opt out from any items they need to opt out of the entire ECS system. In order to make a valid choice the clinician must ensure that the patient is given sufficient information to know what their options are and the consequences of opting out of having an ECS record. If a patient chooses to opt out they must inform their GP practice who will

	record this in the patient's GP medical record and set the opt-out flag which will prevent an ECS dataset being sent to the ECS Store.
Data subject's access rights	Yes Patients can ask their GP practice for a copy of their ECS record. ECS Store Audit logs can provide details of when, and by whom a patient's sensitive personal data was requested during a specified period. If requested, this facility can provide a patient with a list of who has looked at their ECS record.

Should an individual choose to refuse to share or limit the use of his/ her information, the implications of such limitation or refusal must be clearly explained and the discussion clearly recorded in his/ her health record

5.2 Statutory Restrictions on/ Requirements for Sharing Information

Restrictions on sharing

There are a small number of circumstances where specific statutory restrictions on disclosure of information apply:

i) The Human Fertilisation & Embryology Act, 2008, 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 1991 prevent 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 limit 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).
iv) The Gender Recognition Act 2004 - Applicants to the Gender Recognition Panel are required to supply evidence from a medical practitioner in support of their application. As 'protected information' covers all information that would identify a person as being a transsexual, if successful in their application a new health record must be created so that protected information is not disclosed.

Special rules on sharing apply if a dataset holding personal identifiable holds some information that may allude to or fall under one of these categories.

The ECS is unlikely to hold data where statutory restrictions on sharing information apply, unless it is included in the Palliative care Summary with the patients knowledge and consent.

6. INFORMATION ASSETS AND MANAGEMENT

6.1 Information held

The data items held on the system as at 1st April 2011 are listed below along with their NHSS classification.

The initial dataset of patient information to be included in ECS was proposed at the Out of Hours/GP Summary meeting, held on 10th December 2003 at Carronvale House, Larbert and agreed and signed off on 11th June 2004 as follows:

Demographics:

- CHI Number
- Forename, Surname, Previous Surname
- Address & Post Code
- Telephone Number(s)
- Date of Birth (DOB)
- Gender :
- Current GP Practice
- GP contact

Clinical Data:

- Allergies
- Medication – prescribed by the GP and recorded on the GP clinical system. Depending on the system, this should include acute prescriptions from the previous 30 days, and repeat medications which have been prescribed within the previous year, including drug name, dose date and quantity.
  On 10th October 2011 this was redefined to include all active repeat prescriptions and acute medication from the past 3 months. GP practices have the option to include medications prescribed outside Primary Care and these will be present on the ECS record.
  Chronic Medication Service (CMS) prescriptions will include the date dispensed.

Technical Data

- Consent Status
- Registration Status
- Deducted field (indicating patient no longer registered)

Additional Data fields held in ePCS and KIS are provided in Appendix A

6.2 Consent / Opt Out

The Consent Model for ECS consists of two levels:

a. Implied consent for the initial upload of patient information from the GP system
b. Explicit consent to view an individual patient's record

a. 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 (under DPA 1998).
All patients have the choice to 'opt out' of having their Emergency Care Summary information on the ECS Store. In addition, patients can ask that certain parts of their health information be restricted from normal accessing/sharing. It is not possible to exclude some items from the ECS Dataset and not others, so if a patient wishes to opt out from any items they need to opt out of the entire ECS.

In order to make a valid choice the clinician must ensure that the patient is given sufficient information to know what their options are and the consequences of opting out of having an ECS record.

If a patient chooses to opt out they must inform their GP practice who will record this in the patient's GP medical record and set the opt-out flag which will prevent any data being sent to the ECS Store. If consent is withdrawn ECS will display an on-screen message "Patient consent withheld" and show only name and CHI number. No clinical data will be present on the ECS system. Thus the user is made aware that the system knows about that patient, and is made aware of the patient's position on consent.

b. 'Explicit' consent is required from each patient before viewing a record. This consent is either recorded by voice by the call handler in NHS24 or SAS or documented in the user's application. Access can only take place if the patient is present and can give their consent or a parent or carer, who is legally entitled, gives consent on their behalf.

If a patient is unable to give consent due to their condition, e.g. unconscious, confused or ill, then a clinical decision may be made to assume that consent is in the patients best interest. Clinicians should only access ECS records without consent under exceptional circumstances, and only if they can justify that decision on clinical grounds. All accesses made without consent should have details recorded on a 'break glass' form of who made the decision and under what circumstances, and these accesses will be specifically audited.

Individual Health Board ECS Store Access protocols must specify the person responsible for ensuring this happens.

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

For the specific of medicines reconciliation, the consent is implied, given agreement by the patient to the earlier referral letter. However where possible the patient should be asked or made aware out of normal courtesy.

6.3 Information sources for the system

The sole data source for the ECS is the patient GP practice system and NHS Scotland general Practitioners are the Data Controllers in respect of the information they submit to the National ECS Store. The GP practice record is the master record, and changes can only be made to ECS records by updating the GP record. No ECS record should be deleted unless requested by the patient when they 'opt out'

Any updates to the ECS dataset in a patient record will generate an update to the ECS record The GP's system creates a batch file twice a day in XML format which is sent to the ECS interface software and the different dataset components are matched onto the ECS XML schema.

The release of the ECS dataset from the GP system is an automated process which utilises the existing interface used for transmitting data between systems in NHS Scotland – the Partners e-Links package.

The transfer of data between GP systems and the ECS store is compliant with e-GIF and NHS Scotland security standards. The guaranteed forwarding transit of the Practices XML batch file to the ECS system is managed via the Interface application e.g. an amended version of the GP e-links /partners software. The files sent are restricted to permanently registered patients

Manual input of data directly into ECS is not possible.

6.4 Accuracy and consistency in recording personal information

Maintaining accurate records is a vital part of patient care. If records are inaccurate future decisions may be wrong and may harm the patient.

The validation of the patient information is carried out by the GP systems before the upload to the ECS store. No further validation is taken place after the data is transferred. There is no facility to amend, or append to, records in the ECS store. If there are changes in the patient's demographics, medication or allergies then a new record is uploaded from the GP system.

Any error identified by an ECS user should be reported back to the GP practice, and once the information is corrected in the practice system, an update to the ECS record will be submitted when that session's file is subsequently processed.

7. SYSTEM SECURITY AND OPERATION

The Emergency Care Summary system has a System Security Policy (SSP) and a Standard Operating Procedure (SOP) which contain details about the system running and archiving arrangements, in line with the requirements of the NHSS Information Security Policy. These are attached at Appendix B.

8. RECORD KEEPING ARRANGEMENTS

The following arrangements ensure that the ECS system meets the Data Protection Act requirement to hold and dispose of data securely:

There is a requirement to retain all historical data within ECS and all records will be archived after 13 months, and a full audit trail of all accesses maintained Patients who are deducted from their practice will remain on the system until they register with a new practice, when their record will be overwritten with updated details. Any patient who is recorded as being deceased will be removed at date + 3 years.

ECS records of patients who chose to 'opt out' will be deleted. Only the demographic information held in CHI will be retained, with a note of the opt out status.

These arrangements comply with the Scottish Government Records Management: NHS Code of Practice [12] which states that NHS Scotland policy all archived records must be kept for a minimum of six years but in the case of ECS records, these are all copies of information held on primary systems and therefore do not require to be kept for six years.

9. BUSINESS CONTINUITY ARRANGEMENTS

Boards will describe their specific Business Continuity arrangements in respect of the actions to be taken to:

- Minimise disruption
- Ensure that everybody is aware of what is required of them
- Resume normal activity a.s.a.p.

A document has been produced by Atos Origin Alliance outlining the Disaster Recovery procedures to be followed in the event of a failure of the central database. A copy is attached at Appendix B

10. TEST / TRAINING DATABASE ARRANGEMENTS

The use of real patient data for testing / training contravenes the Data Protection Act. In line with good practice[13], the NHSS requires all new systems to have a "test environment" where new developments and upgrades can be tested.

The ECS has 2 separate environments which can be used for testing and training. The test and training environments do not use live patient data and are completely separate from the live infrastructure. It is maintained by Atos Origin and complies with NHSS NISG best practice guidance on this.

11. POLICY DISTRIBUTION

The protocol and any associated documentation will be available to all members of staff in the Organisation and to any appropriate third-party individuals or companies working on behalf of the organisation. The protocol will also be made available on the ECS website.

This Protocol will be reviewed every two years by the ECS service board or more frequently if appropriate to take into account changes to:

- the system,
- the data set
- personnel and/or
- legislation that may occur, and/or guidance from the Scottish Government and/or the UK Information Commissioner.

The review will be conducted in line with existing *SG and NSS IG* procedures and will evaluate the use and effectiveness of this guidance by;

- Obtaining formal feedback from Caldicott Guardians and other members of the Information Governance community.
- Reviewing the outputs from any relevant audit work
- Analysing documentation relating to reported breaches of this guidance

[12] Records Management: NHS Code of Practice (Scotland) Version 2 (2010) ,
[13] BIP 0002:2003 Guidelines for the use of personal data in system testing : http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030100005

- Analysing complaints received by organisations to determine whether they relate to breakdown or inadequacy of the guidance.

APPENDIX A

The Privacy Impact Assessments for ePCS and KIS have been attached for reference here:

ePCS

Privacy Impact Assessment ePCS V1

KIS

2011-09-16 Privacy Impact Assessment -

APPENDIX B

ECS – Disaster Recovery Test Process

C:\InfoGov\ECS
Disaster Recovery Te

ECS - Secure Operating Procedures & System Security Policy

C:\InfoGov\
ECSSOPSSP v1.2.doc