

THE "OPEN EXETER" SYSTEM
MODEL SECURITY POLICY AND RELATED ISSUES

1 INTRODUCTION

1.1 Purpose of the Policy

The purpose of this policy is to :

- 1.1.1 Describe NHS Connecting for Health's expectations about the environment in which the Open Exeter system will be operated.
- 1.1.2 Anticipate and avoid any departure from good practice with regard to security and confidentiality.

1.2 Certification of People Given Access to Open Exeter

There will be three system-wide types of certification, i.e.

1.2.1 Data Controller Certificates

- a) Data Controller Certificates will be issued to persons authorised by Chief Executive Officers (CEOs) to issue Data User Certificates.
- b) Data Controller Certificates may be issued to NHS Trust Caldicott Guardians for control of Data Users' access to data covered by conditions approved under Section 60 of the Health and Social Care Act 2001.
- c) It is assumed that holders of Data Controller Certificates will discharge the duties of a Data Controller as described in the Data Protection Act 1998.

1.2.2 Data User Certificates

- a) Data User Certificates will be issued to persons duly authorised by a Data Controller. These certificates will specify the name of the person, the data to which they have access, and the period for which access is authorised.

1.2.3 System Support Certificates

System Support Certificates will be issued to NHS Connecting for Health's staff who provide:

- a) technical support to the hardware and software that constitutes the "Open Exeter" application and service.
- b) customer support to Data Controllers and Data Users.

1.3 Business Context.

- 1.3.1 The system of certification is of two types - paper based and electronic based.

- 1.3.2 Paper certification is used for Data Controllers. It is assumed that the paper certificates will be joined or replaced by electronic certificates at some time in the future, possibly secured by digital signatures.
- 1.3.3 Data Users may have paper certificates, physically signed by a recognised Data Controller, or have "Open Exeter" accounts electronically generated on-line by recognised Data Controllers. The electronic record of the Data Controller generating or amending the Data User's account is the Data User's electronic certificate.

2 THE MODEL POLICY

Data Controllers should ensure that there are written procedures to cover:

2.1 Verification of Applicants

- 2.1.1 There should be a mechanism for demonstrating the Persons applying for user certificates have a business need to access the data cited in the application.
- 2.1.2 CEOs and Data Controllers should consider the need for vetting applicants for data user certificates (e.g. via subject access requests to police computer systems).

2.2 Generation of Certificates

When issuing user certificates or generating or amending user accounts on-line, Data Controllers should ensure that:

- 2.2.1 the standard application procedure has been followed (e.g., the right form has been used and all the required data and authorisations are present and correct. Standard application forms are available from the NHS Connecting for Health web site, updated as functionality is added to the "Open Exeter" application);
- 2.2.2 the application has been processed in a timely fashion (for example the Data Controller might consider it unwise to endorse an application if a period of several weeks has elapsed since the origination of the application);
- 2.2.3 Data Controllers should consider establishing a maximum elapsed time for the processing of an application in order to prevent inappropriate certification of staff who have left or changed their roles, etc.
- 2.2.4 all authorisations are valid at the time that the Data Controller endorses the certification.
 - a) If a local "in-house" protocol governing the processing of applications calls for applicants to be authorised (by for example the applicant's line manager), then a third, purely local, mechanism for certification of "endorsers" may be needed.
 - b) Checks should be made to ensure that the authorising signatory is duly authorised at the time that the Data User

Certificate is endorsed as well as when the signatory authorised the application.

2.3 Publication of Certificates

The Data Controller should consider:

- 2.3.1 what is the appropriate access to the certificates themselves;
- 2.3.2 how the content of the certificates will be published locally and to other NHS organisations.

Data Controllers should balance the need for security with the operational efficiency of the organisation.

2.4 Revocation of Certificates

- 2.4.1 There must be a mechanism whereby certificates can be revoked in a timely manner when a certificate holder: resigns ; changes their role ; takes maternity leave; takes long term sick leave; or is subject to disciplinary procedures.
- 2.4.2 The revocation procedures should be designed so that, where possible (e.g. where a member of staff gives notice of resignation), revocation can be set to coincide with the data user ceasing the role in which they are certified.

A revocation form is available from NHS Connecting for Health's web site. However, other forms of written request for revocation from Data Controllers will be acceptable. Also, Data Controllers may revoke Data User accounts using the on-line maintenance facility, in which case revocation is instantaneous.

2.5 Expiration of Certificates

- 2.5.1 The maximum duration of a certificate will be 6 calendar months after a password expires without having been reset. (This is to accommodate Data Users who may be absent due to extended periods of illness or maternity leave).
- 2.5.2 There should be a mechanism for giving advance notification of the certificates that are due to expire (for example, where a Data User gives notice of resignation the Data Controller may send a revocation form to NHS Connecting for Health specifying the date upon which the Data User's access to "Open Exeter" will be terminated.)
- 2.5.3 There should be a procedure for formally reviewing the need for a renewal of current certificates (for example, an annual review of an organisation's access).

2.6 Archiving of Certificates

Data Controllers and CEOs should decide for how long lapsed certificates should be stored.

2.7 Audit

- 2.7.1 All organisations should certify at least one Data User with "Caldicott Guardian" access.
- 2.7.2 Using the "Caldicott Guardian" access, a schedule of auditing should be drawn up and executed. It is recommended that sampling queries are used to look for unusually high numbers of queries from a single source, for queries that are inconsistent with the role of the Data User and for unusual times for the system being in use.
- 2.7.3 it is recommended that sample spot check audits are carried out on a weekly basis.

2.8 Contingency

Data Controllers should consider the need for a reserve Data Controller who can be called upon in the absence of the first-line Data Controller. If an organisation has a reserve Data Controller then they should be properly trained.

3 THE ROLE OF NHS CONNECTING FOR HEALTH

NHS Connecting for Health will:

- 3.1 Establish a set of procedures with regards to certification of Data Controllers. These procedures will be published to organisations using "Open Exeter".
- 3.2 Manage the Authorisation of Data Controllers.

Data Controllers can be authorised by the CEO or whoever is deputed by the CEO. NHS Connecting for Health will hold records of up to three authorised signatures for each NHS organisation having custody of an Exeter System (for example, Head of Public Health, Head of Information Systems, Caldicott Guardian).
- 3.3 Manage and maintain the lists of NHS organisations which adopt the schedules to this policy.
- 3.4 Manage and maintain the list of organisations permitted to use Schedule A to this policy. Entry on to this list must be by approval of the Open Exeter Project Board. In the event of the Open Exeter Project Board granting approval for an organisation to use Schedule A, NHS Connecting For Health will notify Data Controllers who have responsibility for granting access to an Exeter System so that consideration may be given to the appropriateness of any access granted.
- 3.5 In the event that the Chief Medical Officer recognises a national pandemic influenza event is occurring, as communicated by Department of Health letter, NHS Connecting for Health will make the Open Exeter Pandemic Flu application available to Data Controllers who have responsibility for granting access to an Exeter System. The provisions of Schedule A will apply.
- 3.6 Produce audit report of changes to certification.

3.7 Manage Authorisation of NHS Connecting for Health staff with access to "Open Exeter".

4 POINTS OF CONSIDERATION

4.1 Community of Trust

4.1.1 There are three Community of Trust models to choose from.

- a) The Hierarchy (I'll only trust you if the boss tells me to) is easy to administer but operationally slow even with computerised support using digital signatures.
- b) The web of trust (any friend of yours is a friend of mine) is operationally fast but is administratively burdensome.
- c) The hybrid. (I trust my family but I wont speak to strangers unless a parent says its OK) is probably the best, technically it is culturally well suited to the NHS, and it is the closest to the current practice. Under this model NHS Connecting for Health sets up a web of trust between Data Controllers and they hierarchically manage their "family".

This model is easily extensible to take in new communities. For example, we could have a GP Data Controller for a Primary Care Trust area so that we could avoid the burden of a controller in every practice. That Data Controller could then deal with the Caldicott Guardian in each practice.

4.2 Initiating the Community of Trust

- 4.2.1 When requested, NHS Connecting for Health will despatch Data Controller certificates to NHS organisations having custody of an Exeter System. These are completed by the CEO of the organisation or their authorised deputy and returned to NHS Connecting for Health. These must contain the sample signature of each authorised Data Controller. The CEO and authorised deputies' signatures should be countersigned.
- 4.2.2 NHS Connecting for Health will hold a register of signatures. These signatures will be checked when Data User certificates requesting access to Open Exeter are received.
- 4.2.3 Additionally, on the Data Controller certificates, CEOs or their authorised deputies may adopt the terms of specific schedules to this model security policy.

4.3 Managing Certification

- 4.3.1 The "Open Exeter" service manager will review NHS Connecting for Health staff System Support Certificates monthly. Where appropriate, access will be revoked or set to expire (for example, where a

member of the System Support staff gives notice of resignation their account should be set to expire when they leave).

- 4.3.2 NHS Connecting for Health must consider vetting staff (e.g. via subject access requests to police computer systems). This recommendation will be considered for a wider range of NHS Connecting for Health staff than "Open Exeter" System Support staff because of NHS Connecting for Health support access to Health Authority and other patient data.
- 4.3.3 Provision of digital certificates within the NHS is being investigated by NHS Connecting for Health. It is anticipated that digital certificates will join or replace paper-based systems in due course, including those used to manage access to the "Open Exeter" application.

Schedule A - NHS-wide Community of Trust

This schedule, (A), to the model security policy covers the Community of Trust between NHS organisations having custody of Exeter Systems and appropriately authorised Data Users in NHS organisations.

- i) This schedule is designed to eliminate multiple Data User Certificates for each individual Data User requiring access to multiple Exeter Systems. This schedule may apply to Data Users in:
- NHS organisations with a NHS-wide remit, e.g., the Prescription Pricing Authority check prescription exemption entitlements throughout England.
 - Large NHS Trusts and tertiary centres which treat patients from large or regional geographical areas.
 - Regional QA Reference Centres which audit screening records.
 - National centres of excellence which treat patients from throughout England.
- ii) In the event that the Chief Medical Officer recognises a national pandemic influenza event is occurring, as communicated by Department of Health letter, this is the schedule which will apply. If not previously revoked, permission for a Data User to use Schedule A for access to data within the Open Exeter Pandemic Flu application will expire automatically after 6 months, whereupon access will be revoked.
- iii) CEOs or their authorised deputies may nominate Data Controllers to the 'Schedule A list', to be held and maintained by NHS Connecting for Health on behalf of all participating NHS organisations having custody of an Exeter System.
- iv) Members of the 'Schedule A list' will have delegated authority to sign Data User Certificates on behalf of all other members of the list when:

- the Data User's NHS organisation is on the list of organisations approved by the Open Exeter Project Board to use Schedule A;
- the Data User's NHS organisation is physically located in their area;
- the Data User is granted equal or greater access to their 'home' Exeter System by the Data Controller.

Schedule B - NHS-wide Breast Screening Investigations

This schedule, (B), to the model security policy covers the Community of Trust between NHS organisations having custody of Exeter Systems and appropriately authorised Data Users undertaking urgent and emergency investigation of breast screening records.

- i) This schedule is designed to facilitate failsafe and clinical audit by the elimination of multiple Data User Certificates for each individual Data User requiring access to multiple Exeter Systems in order to check the breast screening records of patients.
- ii) CEOs or their authorised deputies may nominate Data Controllers to the 'Schedule B list', to be held and maintained by NHS Connecting for Health on behalf of all participating NHS organisations having custody of an Exeter System.
- iii) Members of the 'Schedule B list' will have delegated authority to sign Data User Certificates on behalf of all other members of the list when:
 - the Data User is undertaking an urgent and emergency investigation into breast screening records;
 - the Data User 's NHS organisation is physically located in their area;
 - the Data User is granted equal or greater access to their 'home' Exeter System by the Data Controller;
 - the Data User is granted access only to the records of female Data Subjects;
 - the Data User is granted access to breast screening records.
- iv) Additionally, the National Co-ordinator for NHS Cancer Screening Programmes will be a member of the 'Schedule B list' and will have delegated authority to sign Data User Certificates on behalf of all other members of the list;
- v) If not previously revoked, permission for a Data User to use Schedule B will expire automatically after 6 months, whereupon access will be revoked.

Schedule C - NHS-wide Cervical Screening Investigations

This schedule, (C), to the model security policy covers the Community of Trust between NHS organisations having custody of Exeter Systems and appropriately authorised Data Users undertaking urgent and emergency investigation of cervical cytology records.

- i) This schedule is designed to facilitate failsafe and clinical audit by the elimination of multiple Data User Certificates for each individual Data User requiring access to multiple Exeter Systems in order to check the cervical cytology records of patients.
- ii) CEOs or their authorised deputies may nominate Data Controllers to the 'Schedule C list', to be held and maintained by NHS Connecting for Health on behalf of all participating NHS organisations having custody of an Exeter System.
- iii) Members of the 'Schedule C list' will have delegated authority to sign Data User Certificates on behalf of all other members of the list when:
 - the Data User is undertaking an urgent and emergency investigation into cervical cytology records;
 - the Data User 's NHS organisation is physically located in their area;
 - the Data User is granted equal or greater access to their 'home' Exeter System by the Data Controller;
 - the Data User is granted access only to the records of female Data Subjects;
 - the Data User is granted access to cervical cytology records.
- iv) Additionally, the National Co-ordinator for NHS Cancer Screening Programmes will be a member of the 'Schedule C list' and will have delegated authority to sign Data User Certificates on behalf of all other members of the list.;
- v) If not previously revoked, permission for a Data User to use Schedule C will expire automatically after 6 months, whereupon access will be revoked.

Schedule D - NHS-wide Ophthalmic Payments

This schedule, (D), to the model security policy covers the Community of Trust between NHS organisations having custody of Exeter Systems and appropriately authorised Data Users in NHS organisations making payments to ophthalmic contractors.

- i) This schedule is designed to eliminate multiple Data User Certificates for each individual Data User requiring access to multiple Exeter Systems in order to verify the entitlement of ophthalmic claims:
- NHS organisations which make payments to ophthalmic contractors receive GOS claims for payment in respect of patients who may be recorded on any Exeter System. (The patient has complete choice as to which ophthalmic practitioner they visit). However, the ophthalmic practitioner submits claims for payment to the NHS organisation in whose area their premises are located.
 - In order to verify the entitlement of the patient to the service claimed by the ophthalmic practitioner, the NHS organisation making payment may need to check the patient's details on the Exeter System wherein the patient's details are recorded.
- ii) CEOs or their authorised deputies may nominate Data Controllers to the 'Schedule D list', to be held and maintained by NHS Connecting for Health on behalf of all participating NHS organisations having custody of an Exeter System.
- iii) Members of the 'Schedule D list' will have delegated authority to sign Data User Certificates on behalf of all other members of the list when:
- the Data User is involved in the processing of claims for payment of ophthalmic services;
 - the Data User 's NHS organisation is physically located in their area;
 - the Data User is granted equal or greater access to their 'home' Exeter System by the Data Controller.