Remote Data Extraction Policy and Procedure

Prepared by PRIMIS

June 2015

Contents

1. Introduction

1.1. PRIMIS activities aim to support primary care researchers and healthcare staff in data extraction and analysis, and improving data quality and information management. This policy explains how PRIMIS provides robust IG procedures for remote data extraction from GP Practices to ensure the delivery of internal IG assurance in accordance with national operating frameworks, legislation and the NHS IG Toolkit.

1.2. Information Governance (IG) practice allows PRIMIS and individual members of staff to ensure that information (including personal and sensitive information) is handled legally, securely, efficiently and effectively and to support the efficient location and retrieval of records where and when needed.

1.3. This policy should be read alongside the PRIMIS I.G. Policy (v1.0), PRIMIS practice data security and confidentiality (v2.0) and PRIMIS Data Sharing Agreements (DSA) Policy and Procedure (v2.0).

2. Purpose and scope

2.1 This policy identifies the principles and procedures required to ensure that all PRIMIS employees and commissioned contractors (Clinical Director and Clinical Associates) comply with the law and best practice when carrying out remote data extractions from GP practice clinical systems.

2.2 The principles cover all aspects of information handling and transmission carried out remotely (including MIQUEST data extractions, CHART audits, saving or archiving search results, mail-merge).

3. Policy Statement

3.1. PRIMIS acknowledges that it must demonstrate to third parties its commitment to ensuring the security of GP practice data and systems. The objectives of this policy are to:

- provide an organisational procedure in which potential security and confidentiality threats resulting from the use of third party remote access software can be identified, mitigated and managed
- illustrate the commitment of the PRIMIS Senior Management Team (SMT) to the security of information and associated systems
- provide clearly stated principles of IG to facilitate consistent compliance with IG standards across the organisation

4. Responsibilities and Compliance

4.1 The PRIMIS Senior Management Team (SMT) is committed to ensuring compliance in accordance with this policy.

- The ***Managing Director*** has overall responsibility (at a strategic level) for ensuring satisfactory compliance with data extraction policy and procedures.
- This responsibility is delegated (at an operational level) to the ***Head of Operations*** (in the capacity as the ***IG lead*** for PRIMIS) and to the ***Information and Software Development Manager*** (in the capacity of ***Caldicott Guardian*** for PRIMIS).
- The ***IG Lead*** will be responsible for regular review and maintenance of this policy.
- The ***IG Sub-committee*** will be required to approve the initial version of the policy and any subsequent versions arising as a result of significant changes to process and scope.
- A***ll staff, contractors and third parties*** will be required to comply with this policy and supporting standards and procedures, where appropriate.

5. Principles of Remote Data Extraction security and confidentiality

5.1 Only third party software approved by the PRIMIS IG Sub-committee can be used for remote data extraction at GP practices. This will generally be the 'Away from my Desk' (AfmD) application.

5.2 Where a customer uses a different locally approved remote data extraction application and requires PRIMIS to use this software for remote data extractions, an application must be submitted to PRIMIS and will require approval by the PRIMIS IG Lead and Caldicott Guardian.

5.3 A log (the RDE log) will be kept at PRIMIS to record the date and time of access, name of PRIMIS staff member, the software application used, which console was used (where applicable), name of practice and name of practice contact. This log is audited bi-monthly by the Head of Operations.

5.4 Before any remote data extractions can take place, practices must agree to the PRIMIS Remote Data Extraction (RDE) Agreement (see Appendix 1). The only exception is in the case of the helpdesk where a practice can give permission for immediate access to resolve a technical issue. In such cases, a record must be kept in the RDE log that the process was explained to the practice and the name of the staff member who granted permission to access (refer to 5.5).

5.5 The person undertaking the RDE makes an entry in the RDE log confirming that a practice agreement has been received, under the column titled 'Practice Agreement'. If carrying out a RDE that has been booked via the voucher system, where the agreement is accepted as part of the booking process, VS should recorded under this column. If the RDE is being carried out at the request of the practice contacting the helpdesk, HD should be recorded in the column, together with the name of the staff member who granted permission to access.

If the RDE session has been arranged because PRIMIS is testing or piloting data extraction tools or processes, TP should be recorded in the log. In all other instances, which is typically as part of a research project, the person undertaking the RDE should be aware of the status of the agreement and should record Y in the log to confirm that the agreement has been accepted by the practice. No PRIMIS member of staff is permitted to remotely dial into a practice's system without the practice having accepted the relevant PRIMIS Remote Data Extraction (RDE) Agreement.

5.6 Practices must create a unique PRIMIS user account on the clinical system only giving access to MIQUEST. Practices should ensure the integrity of the practice audit trail through identification of the user as a member of PRIMIS staff. All actions undertaken by PRIMIS on the practice system can be monitored on-screen by the user at the practice. The user at the practice can terminate connection at any point during remote access.

5.7 Practices are responsible for ensuring that only the MIQUEST interpreter is visible to PRIMIS staff. The patient record must be closed, to ensure that no access is possible to patient identifiable information.

5.8 On occasions, the RDE session may require data transfer to PRIMIS. Data are transferred using the data transfer facility within remote access software. AfmD has inherent security processes via an encrypted computer link (Secure Socket Layer (SSL) link).

5.8.1 As part of the voucher system service, where the practice has requested that their pseudonymised data be uploaded to the CHART Online data warehouse. In such instances, the practice has agreed to the transfer as part of their booking of the service. Where one-line-per-patient de-identified data is being uploaded, the practice is required to accept a Data Collection/Sharing Agreement (DCA/ DSA) specific to the project.

5.8.2 During the testing or piloting of a data extraction tool or process, a problem may be encountered that requires a more detailed review of the data outputs (for validation or de-bugging purposes). In such cases, the permission of the practice to remove the aggregate or one-line-per patient de-identifiable data during the RDE session will be sought and recorded on both the RDE and test log. Under no circumstances are PRIMIS staff permitted to transfer patient identifiable data. Refer to the PRIMIS policy for Testing and piloting data extraction tools and processes in general practice (v1.2) for more detailed information.

5.8.3 During a project whereby it has been agreed with the customer that pseudonymised data will be transferred to PRIMIS (other than data transfer to CHART Online). In such cases, the practice is required to accept a DCA/ DSA specific to the project.

5.9 In exceptional circumstances where a customer or practice requests the extraction of patient identifiable data or creation of a mail-merge facility during the RDE session, this will only be carried out with the explicit permission of the practice and will be recorded in the RDE log. In the case of the creation of a mail merge facility, the PRIMIS member of staff will create a spreadsheet containing named patient data in order to produce a mail merge file. All files will be created and saved onto a safe location agreed with the practice. It is recommended that the practice consider deletion of these files once the mail merge letters have been printed and sent out to patients. Practices requesting PRIMIS to create the mail-merge facility must accept the PRIMIS mail-merge agreement (refer to PRIMIS Data Sharing Agreement Policy v2.0).

6. Incident Management

6.1 All incidents involving breaches of confidentiality or data loss will be managed through PRIMIS's ISO 27001 Information Security Management System 'non-conformity' incident reporting procedure. The Head of Operations, in their role of Information Governance Lead for PRIMIS will co-ordinate the investigation and response to all such incidents and be responsible for identifying, implementing and reporting on associated corrective actions. The Head of Operations monitors performance against the non-conformity/corrective action process. All incidents are reported to the PRIMIS IG Sub Committee, which monitors the response.

7. Training/Awareness

7.1 PRIMIS requires that all employees and contractors attain and maintain an acceptable degree of IG awareness. All staff using remote access software must be introduced to this policy and given training and awareness on remote access procedures (outlined in the RDE Practice Agreement in Appendix 1).

8. Distribution

8.1 Once approved, this policy is to be distributed to all staff and contractors and posted on the PRIMIS SharePoint (Intranet) site for future reference. Subsequent changes to the policy will be version controlled and shared with PRIMIS staff and contractors.

Appendix One: PRIMIS Practice Agreement for Remote Access

(Highlighted areas to be completed/ deleted as appropriate)

Thank you for agreeing for PRIMIS to remotely access your clinical system. As part of the process, PRIMIS will use the 'Away from my Desk' software to enable remote running of MIQUEST queries on the practice clinical system MIQUEST interpreter. To ensure the security of your data, PRIMIS has developed the following terms of access which must be followed at all times.

During the [period of project/dates/testing period] the practice agrees to:

1 Allow PRIMIS to remotely access their computer system in accordance with the attached procedure at agreed dates and times [purpose of access: e.g. to assist in the quality control of MIQUEST query library development/to allow collection of data for the XXXXXX project/ remote installation and support].

2 Ensure that appropriate security and confidentiality procedures are observed at all times.

3 Allow PRIMIS staff to access extracted data for the purposes covered by the project documentation.

Access Process:

- A member of the PRIMIS team will contact the practice to arrange a date and time for data collection (two dates will be required for practices using EMIS Web or EMIS PCS where MIQUEST queries run overnight).
- On the agreed dates, a member of the PRIMIS Team will access the MIQUEST Interpreter on the practice clinical system using the 'Away from my Desk' application.
- System access times will be kept to a minimum.

Please note the relevant desktop computer at the practice cannot be used by any member of practice staff while a remote access connection is in place.

Confidentiality and security:

- The 'Away from my Desk' software used to gain access must be authorised by a user at the practice before a connection can be made by PRIMIS. PRIMIS cannot access the practice systems without explicit authorisation. Instructions on how to give authorisation will be supplied on request.
- The 'Away from my Desk' software has been specifically developed to comply with the strict rules laid out within the NHS Information Governance Toolkit and has fully-compliant audit trail logging.
- All actions undertaken by PRIMIS on the practice system can be monitored on-screen by the user at the practice. The user at the practice can terminate connection at any point during remote access.

- Only the MIQUEST interpreter will be visible to PRIMIS staff. The patient record will be closed, to ensure that no access is possible to patient identifiable information.
- Practices should create a unique PRIMIS user account. It is not necessary to inform PRIMIS of the detail, but the account should only give access to MIQUEST, and ensure the integrity of the practice audit trail through identification of the user as a member of PRIMIS staff.
- If unexpected access to confidential information occurs during the course of accessing the practice system, that information will not be disclosed to any other person. This condition applies during time working with the practice and after that ceases.
- A log file will be kept at PRIMIS recording which individual staff member used the 'Away From My Desk' software to remotely access the practice system in each case.
- During the period of access, the practice agrees to:
  - allow PRIMIS to remotely access their computer system in accordance with the procedure described above at agreed dates and times
  - ensure that appropriate security and confidentiality procedures are observed at all times
- In exceptional circumstances where a practice requires support from PRIMIS that involves extraction of patient identifiable data or creation of a mail-merge facility, this will only be carried out with the explicit permission of the practice and will be recorded on the PRIMIS log. No patient identifiable data will be removed from the practice under any circumstances.
- Access to the practice computer system by PRIMIS staff can be terminated at any time by either the Practice or PRIMIS.

Appendix Two: PRIMIS Practice Agreement for Remote Access: Northern Ireland

(Highlighted areas to be completed/ deleted as appropriate)

Thank you for agreeing for PRIMIS to remotely access your clinical system. As part of the process, PRIMIS will use the 'BOMGAR' software to enable remote running of MIQUEST queries on the practice clinical system MIQUEST interpreter. To ensure the security of your data, PRIMIS has developed the following terms of access which must be followed at all times.

During the [period of project/dates/testing period] the practice agrees to:

1 Allow PRIMIS to remotely access their computer system in accordance with the attached procedure at agreed dates and times [purpose of access: e.g. to assist in the quality control of MIQUEST query library development/to allow collection of data for the XXXXXX project/ remote installation and support].

2 Ensure that appropriate security and confidentiality procedures are observed at all times.

3 Allow PRIMIS staff to access extracted data for the purposes covered by the project documentation.

Access Process:

- A member of the PRIMIS team will contact the designated person at the practice to arrange a date and time to run the audits (two dates will be required for practices using EMIS PCS or MERLOCK where MIQUEST queries run overnight).

- On the agreed dates, a member of the PRIMIS Team will require access to the MIQUEST Interpreter on the practice clinical system and to a designated practice desktop computer using the BOMGAR application.

- PRIMIS will then use the BOMGAR software to:
  - download, install and configure CHART onto the designated desktop agreed with the practice
  - download and install the specified audits and run both anonymised and patient identifiable MIQUEST queries on the practice clinical system
  - transfer the results to CHART and then archive them if required
  - add a new folder to the desktop called PRIMIS information
  - store the following in the folder:
    - CHART and MIQUEST instructions
    - data interpretation and analysis booklet(s) where available
    - details of how and where to access the results of the audits

System access times will be kept to a minimum

Please note the designated computer at the practice cannot be used by any member of practice staff while a remote access connection is in place

Confidentiality and security:

- The BOMGAR software used to gain access must be authorised by a designated user at the practice before a connection can be made. PRIMIS cannot access the practice systems without explicit authorisation.

- The BOMGAR software has been approved for use by the Northern Ireland Health and Social Care Board and has fully compliant audit trail logging.

- All actions undertaken by PRIMIS on the practice system can be monitored on-screen by the user at the practice. Practices are advised to observe on the screen what happens during the connection. The user at the practice can terminate connection at any point during remote access.

- Only the MIQUEST interpreter will be visible to PRIMIS staff. The patient record and consultation screens will be closed, to ensure that no access is possible to patient identifiable information.

- Practices should create a unique PRIMIS user account on their computer. It is not necessary to inform PRIMIS of the detail, but the account should only give access to MIQUEST, and ensure the integrity of the practice audit trail through identification of the user as a member of PRIMIS staff.

- If unexpected access to confidential information occurs during the course of accessing the practice system, that information will not be disclosed to any other person. This condition applies during time working with the practice and after that ceases.

- A log file will be kept at PRIMIS recording which individual staff member used the BOMGAR software to remotely access the practice system in each case.

- During the period of access, the practice agrees to:
    - allow PRIMIS to remotely access their computer system in accordance with the procedure described above at agreed dates and times
    - ensure that appropriate security and confidentiality procedures are observed at all times.

- No patient identifiable data will be removed from the practice under any circumstances.

- Access to the practice computer system by PRIMIS staff can be terminated by either the Practice or PRIMIS.

- In the event of any security incident, including breaches of confidentiality and data loss, PRIMIS are required to inform the practice, and at the same time inform the Northern Ireland Health and Social Care Board. Depending on the severity of the incident senior management at PRIMIS may also be required to bring the general details of the incident to the attention of the PRIMIS Information Governance sub-committee in line with PRIMIS internal policies.

Appendix Three: Mail-Merge Agreement

[Name of Project]

Mail-merge Agreement

Practice Name: ____

Practice National Code: ____

Address: ____

____

Contact Name: ______________________ Email: ______________

Title: ______________________ Telephone: ______________

By accepting this agreement, you are permitting a PRIMIS member of staff to use the CHART software tool to view and sort named patient data for the purpose of creating mail-merge letters.

The following process will be followed:

1. The PRIMIS member of staff will log onto the practice PC to carry out the data extraction and transfer processes, specific to the project.
2. A folder is created to store the named response files, which should be in a secure location.
3. Once the audit has been run, the response files are exported to the appropriate folder (see 2).
4. The response files containing named patient data are deleted from the clinical system.
5. The response file is loaded into CHART to create a spread sheet that contains the data in the datasheet (i.e. patient name, Read codes and addresses).
6. If required, the spread sheet is filtered to remove patients outside the relevant search criteria and those with an exclusion code in their record.
7. The file is opened to check that the criterion has been applied correctly and that the address columns have been populated. Once checked, the file is then closed.
8. The mail merge letter is then opened and the mail merge wizard used to create a file containing a letter for each patient.

The PRIMIS member of staff will only have access to patient identifiable data during the process described above and for the stated purposes. No patient identifiable data will be removed from the practice under any circumstances.

While PRIMIS can create a mail-merge file to identify patients who meet specific criteria, it remains the responsibility of the practice to ensure that letters are not sent inappropriately to any patient.