Document title	FFFAP data sharing policies and procedures
Version	1.2
Date	April 2016
Authors	Chris Boulton, Rowena Schoo
Approved by	Roz Stanley FFFAP Programme Manager
Review Date	April 2017

This document describes FFFAP guidelines in the sharing of data and sensitive information. It is intended to reflect most common occurrences; however, we acknowledge that frequent unusual circumstances occur in our field of work, and decision will often need to be made on a case-by-case basis.

For advice on flows of data or information, please see Roz Stanley, FFFAP programme manager or Chris Boulton, NHFD project manager.

Personal data

Link to summary table

The programme is not authorised to handle or process personal (patient level, identifiable) data in any form. If you are sent data in this format from a participant site, supplier or third party. Please do the following…

1. Instruct the sender that FFFAP are not legally entitled to receive or otherwise process patient identifiable information and advise the correct way to enter such data if appropriate
2. Destroy the data in a secure manner.
    a. For electronic receipt
        i. Delete the email
        ii. Go to your trash and press delete again and select 'yes' to permanently delete the email
    b. For hard copies received
        i. Dispose of the paper in the secure disposal (white bags located in each office)
3. Inform the project manager responsible for the appropriate audit workstream (or the programme manager if it a programme-wide event).
4. Project managers to inform programme manager of any such occurrences so that a decision can made as to whether an RCP incident procedure needs to be initiated.

Limited access anonymised data for routine work

Link to summary table

FFFAP team

It is entirely acceptable for the FFFAP team to hold limited access anonymised (non-identifiable patient level data) for the purposes of management of the workstreams, analysis and report writing. Patient level data can be sensitive, even if hard identifiers have been removed. Care should be taken when handling.

- Data from FFFAP webtools should only be received directly from Crown Informatics using a secure file transfer, and with the authority of the project or programme manager.
- Data should be kept in a csv or xls format, password protected and saved in the FFFAP folders of the network storage area.
- Data should be accessed on the network drive by the FFFAP team. It should not be moved or copied to PCs, laptops or personal network drives without the authority of the programme or project managers.
- Data files should not be sent via email – even to other members of the team.

Persons authorised to access data under this process are:

- FFFAP programme manager
- FFFAP project managers
- FFFAP project coordinators
- FFFAP data coordinator
- FFFAP administrator

Clinical leads

FFFAP clinical leads wishing to carry out ad hoc analyses on patient level audit data should discuss their requirements with their project manager in the first instance. The objectives of the project should be fully stated in a (one side of A4) document including details of the data items requested and the planned outputs.

Project managers should check that this is satisfactory from a strategic perspective, prior to an information governance review. Data may only be released following sign of by the project manager and programme manager or IG lead.

When authorised data can be transferred via one of the following mechanisms:

- Secure file transfer using the Crown informatics portal
- Password protected filed via FFFAP workstream Sharepoint sites
- Encrypted email transfer using minimum AES 256 bit standard

Persons authorised to access data under this process are:

- FFFAP clinical lead

- FFFAP workstream clinical leads

Any other parties wishing to carry out analysis using FFFAP patient-level data should apply via the FFFAP scientific and publications committee. Non-executive advisory group members may not access patient level data for the purposes of supporting data analysis.

Anonymised-level data for routine work

Link to summary table

It is entirely acceptable for the FFFAP team to hold aggregated hospital or CCG level data for the purposes of management of the workstreams, analysis and report writing. Aggregated, hospital or CCG level data can be sensitive, even at this level of granularity. Care should be taken when handling any documents that contain information that has not been published.

- Documents containing unpublished findings should be kept in an appropriate file format, password protected and saved in the FFFAP folders of the network storage area.
- Documents should be accessed on the network drive by the FFFAP team. It should not be moved or copied to PCs, laptops or personal network drives without the authority of the programme or project managers. This is to ensure that documents are available in the vent of team absence and to ensure adequate version control.

It will be necessary to share unpublished findings with clinical leads, project teams and other stakeholders for the purposes of writing and compiling reports.

Where it is not necessary for the identity of hospitals to be disclosed for the purposes of writing or contributing to a report, documents should ideally be redacted using Adobe Acrobat software and password protected prior to sharing. Documents may also be watermarked as confidential and draft as appropriate. Redacted password protected documents may be sent via a normal email client.

Where it is not possible to redact the identities of hospitals because this will inform the writing of the report, then sharing must be via one of the following means.

- Secure file transfer using the Crown informatics portal
- Password protected filed via FFFAP workstream Sharepoint sites
- Encrypted email transfer using minimum AES 256 bit standard

Persons authorised to access data under this process are:

- FFFAP programme manager
- FFFAP project managers
- FFFAP project coordinators
- FFFAP data coordinator
- FFFAP administrator

- FFFAP clinical lead
- FFFAP workstream clinical leads
- Crown Informatics team
- RCS-CEU team
- Members of workstream advisory groups
- Members of the FFFAP board
- Other stakeholders as discussed with the project or programme manager

In all circumstances, the sensitivity of data should be emphasised to the recipients and embargoes clearly denoted in the accompanying email.

Password should always be sent under separate email cover form the document that they refer to.

Anonymised data for non-routine work

Link to summary table

FFFAP clinical leads wishing to carry out ad hoc analyses on unpublished hospital level audit data should discuss their requirements with their project manager in the first instance. The objectives of the project should be fully stated in a (one side of A4) document including details of the data items requested and the planned outputs.

Project managers should check that this is satisfactory from a strategic perspective, prior to an information governance review. Data may only be released following sign of by the project manager and programme IG lead.

When authorised data can be transferred via one of the following mechanisms:

- Secure file transfer using the Crown informatics portal
- Password protected filed via FFFAP workstream Sharepoint sites
- Encrypted email transfer using minimum AES 256 bit standard

Persons authorised to access data under this process are:

- FFFAP clinical lead
- FFFAP workstream clinical leads

Data referring to a specific time period may not be elsewhere published until after an RCP authored report reflecting that period has been published.

Unpublished anonymised data for third parties

Under certain circumstances, the release of unpublished, anonymised data may be released to third parties (for example to support BOA site reviews). This needs to be agreed by HQIP and should be discussed with the relevant project manager in the first instance.

Sharing of passwords

Passwords should be sent via email under separate cover to the parent document.

Passwords should contain a mixture of letters and numbers.

Unpublished hospital level information may be password protected using a standard, memorable password such as **fffap2016**

Patient level data files must always have a unique password in a non-standard format

A register of passwords may be kept in a secure, encrypted location on the FFFAP drive with limited access.

Definitions

Personal data is defined here as data which contains direct, 'hard' identifiers for any individual patient – living or dead. Example of identifiers are: Name; Address; Date of birth; Postcode; Date of death.

Patient-level data is defined here as any data files which contains a record which relates to an individual patient, even if that patient is not identifiable, for example, a line of data in an excel Spreadsheet that relates to an individual patient's care recorded in an audit database.

Limited access anonymised is defined here as patient-level data that has had 'hard' identifiers removed, but may still be used to identify individuals using another data source, such as the Crown database or hospital systems.

Anonymised data is defined here as aggregated results or findings related to the performance of a specific hospital, CCG or other equivalent geographic structure.

Summary of types data and protection requirements

Type of data	What does it look like?	Sharing within FFFAP	Sharing with Clinical leads	Sharing with other external parties (AG etc)
Personal data	Personal data is sensitive patient level identifiable data – you can identify the individual (personal data) and it contains information about their health (which makes it sensitive). The most obvious personal information is: name, address, date of birth, postcode, date of death	We do not have permission to handle personal data. If you receive patient identifiable data, see Patient identifiable data for instructions.		
Limited access anonymised data	Health data presented at an individual patient level, but it contains no identifiers: Must not have any of the following: name, address, date of birth, postcode date of death Or any combination of which could allow for the patient to be identified.	Yes, but see transferring and storage requirements.	Yes, but project manager needs to approve. See transfer requirements.	Not permitted
Anonymised data for routine work	Health data presented at a hospital or CCG level, but it contains no identifiers.	Yes, but see transferring and storage requirements.	Yes, but only when hospital / CCG level identification is necessary for the purposes of writing or contributing to a report. See transferring and storage requirements.	
Anonymised data for non-routine work	Health data presented at a hospital or CCG level, but it contains no identifiers.	Yes, but project manager needs to approve. See transfer and storage requirements.		Only published findings.