Document filename:	**NHS Digital CAP Information Security**		
Directorate / Programme	**Data, Insights and Statistics**		
Document Reference	**n/a**		
Project Manager	**n/a**	Status	**Final**
Owner	**Chris Dew**	Version	**1.1**
Author	**Alex Newsome**	Version issue date	**02/08/2018**

NHS Digital Clinical Audit Platform Information Security

Document Management

Revision History

Version	Date	Summary of Changes
0.1	29/12/2015	Initial document creation.
0.2	30/12/2015	Updated to clarify what information can be seen and approach to backups.
0.3	23/09/2016	Updated with additional questions and re-branding.
1.0	23/11/2016	Published following approval.
1.1	02/08/2018	Updated following review and addition of GDPR section.

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Alison Roe	Operations Manager	06/10/2016	0.3
Barbara Stearn	Clinical Audit Co-ordinator	30/12/2015	0.1
Alison Roe	Senior Business and Operational Delivery Manager	31/07/2018	1.0

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Alyson Whitmarsh	Programme Manager	22/11/2016	0.3
Chris Dew	Information Analysis Lead Manager	02/08/2018	1.1

Glossary of Terms

Term / Abbreviation	What it stands for
CAP	Clinical Audit Platform

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1 Introduction

1.1 Purpose of Document

The purpose of this document is to provide an overview of the information security controls that are in place to safeguard the confidentiality, availability and integrity of the Clinical Audit Platform (CAP).

This document is aimed at users of CAP – both internal and external – should they wish to know about the controls in place.

1.2 Background

The Clinical Audit Platform (CAP) is a system used to collect secondary use data for audits, registries or collections that NHS Digital is contracted for. It holds patient confidential data (identifiable data) that is collected under appropriate legal gateways such as Section 251 or Directions under the 2012 Health and Social Care Act.

CAP has separate areas for different audits / registries / collections, allowing different information and functionality to be available to meet the specific requirements of that audit / registry / collection.

2 Frequently Asked Questions

2.1 How do you ensure only authorised people can access data in CAP?

Access to CAP is provided only on receipt of a valid registration form which needs to be sent from the organisation's registered Caldicott Guardian. The users are assigned to the audit / registry / collection and the organisation that the Caldicott Guardian has approved, to ensure they are presented only with data relating to a patient they have a legitimate relationship with. Access requires a unique NHS Digital single sign on account.

The Caldicott Guardian authorisation means that local data processes and security has been applied, so NHS Digital do not place additional clearance on top of the Caldicott arrangements.

Role-based access control ensures users cannot access / alter areas they are not authorised to do so.

2.2 Are there any exceptions to this registration process?

There are some audits which do not contain patient identifiable data and therefore there is no requirement for Caldicott Guardian approval. These audits have other registration controls in place to ensure that users are authorised to access this area of CAP. For example, a 'Nominated' user could be set up if they have a specific NHS email address and they can then add other users and manage the access.

There are some audits which only require users to send data in and CAP does not provide any identifiable data back to the user. These also do not require Caldicott Guardian

approval and have the concept of a 'Primary' user that can be set up if they have a specific NHS email address and they can then add other users and manage the access.

For one audit where GP Practices are registering, a senior partner can approve access in place of the Caldicott Guardian.

Access is provided on a per audit / registry / collection basis i.e. a user does not automatically get the same access to other audits / registries / collections just because they have been authorised for one.

2.3 Can generic accounts be used to access CAP?

Generic or shared accounts should not be used to access CAP. It is important that every account is the responsibility of one individual so that we know what actions have been undertaken in CAP by which person. However, in some instances this is not always possible due to the local organisation set up. Where this is not possible, NHS Digital review requests on a case by case basis

2.4 Can non-professional accounts be used to access CAP e.g. @gmail, @yahoo?

Professional addresses should be used to access CAP as the security of these accounts can then be traced to a particular organisation. However, in some instances this is not always possible due to the roles of people who are submitting to a particular audit / registry / collection. Where this is not possible, NHS Digital review requests on a case by case basis.

2.5 Is there a limit to the number of individuals who can register for CAP access within an organisation?

No. Everyone must be individually registered and typically most organisations register 2-3 people so that there is cover.

2.6 Once individuals are CAP registered, do they only have access to the data which they themselves are submitting currently and / or have submitted in the past specific to the current employing organisation?

Users will have access to data that they have submitted / updated at their current organisation, or that has been submitted by other CAP registered colleagues within the same organisation. If their patient has been seen elsewhere and that has been updated in CAP against the patient record, then they will also be able to see that contact.

2.7 Once individuals are CAP registered, do they have access to any data which they themselves have submitted in the past on behalf of prior employing organisations?

When a user moves organisations, it is their responsibility to inform NHS Digital so that their access to their previous organisation is removed. Should they require access at their new organisation, they will need to submit a new registration for approval by the organisation's Caldicott Guardian.

2.8 Can a user with authorised access search on any NHS number and return details for a patient who they would not have a direct legitimate relationship with, for clarification someone who is not their patient?

CAP allows a registered user to enter a full NHS number that they know and they can then view the record, so if a registered user has access to the NHS number but no legitimate relationship with the patient they can access the record (assuming that record has been inputted by someone into CAP). How much of that record the user can see will depend on the configuration of that audit / registry / collection.

This functionality is in place since a patient can receive care at different organisations and therefore users with approval to access the system at different organisations can submit and view data for that patient. CAP does not have search functionality for NHS numbers; users must put in an exact NHS number for a patient and a result will only be returned if that patient is already in the tool for that audit and the user would need to be registered to access that audit.

2.9 Who else will have access to CAP?

For the online database, NHS Digital technical staff will access this for system maintenance and user support. This is controlled via a clear data access approval process to ensure access is given and removed appropriately.

2.10 What audit controls are available to the organisations (e.g. GPs/Trusts) inputting data into CAP?

CAP records the following actions taken by any registered user (the username / the organisation they are registered to in CAP / date & time):

- Deletion
- Created
- Last updated
- Upload

There is a ‘view history’ option against each record which allows a user to see the ‘Created’ and ‘Last Updated’ information.

2.11 How can organisations meet the requirements of the care record guarantee to show who has viewed what information within the tool?

CAP currently does not record who has viewed information within the tool. We have carried out a review of the overall auditing functionality and processes and have identified the improvements we can make around this, one of which would be to log who has accessed any record within the tool. We are working on a roadmap of these improvements so we can enhance this aspect of the tool.

2.12 Is monitoring undertaken which would highlight suspicious activity to the data controllers i.e. access for an extended period where lots of NHS numbers have been searched on?

We currently do not have monitoring around suspicious activity but have reviewed the approach we can take on this. Our initial step is to improve the auditing functionality within the tool, so we have a wider range of activity data.

We need to determine what may be considered suspicious activity and how this could be applied to our range of audits. Our different audits have varying behaviours which we would need to consider, for example, a high number of records being accessed close to an audit submission deadline would be quite legitimate behaviour.

2.13 Where will the data be stored?

Data entered onto CAP will be held on database servers located within NHS Digital secure data centre facilities.

2.14 Is data entered onto CAP held on a computer?

CAP does not save any data locally on a computer; it is a secure web-based portal. All data will be transferred over HTTPS and therefore encrypted between users and the CAP system.

2.15 How long will the data be stored?

All data submitted to the CAP database will be retained for the duration of the audit / registry / collection and for a minimum of 5 years after closure. To preserve the integrity of system backups, data is not deleted from central backups. It will not be possible to retrieve this data without an authorised reason to do so.

2.16 At the end of this period, how will the data be disposed of?

The data submitted to NHS Digital via CAP will be deleted from the databases that support CAP.

2.17 Who will be responsible for ensuring that the data is disposed of in a confidential manner?

For the data held by NHS Digital in CAP, NHS Digital will be responsible for the secure disposal.

2.18 CAP and the General Data Protection Regulation (GDPR)

CAP is the application used to collect data for audits / registries / collections. Each audit / registry / collection has its own legal basis and CAP holds email addresses for registered users under a specific legal basis.

Email addresses are added into CAP once a validated registration form has been submitted by a user, or they have completed the online registration directly themselves. These email addresses are used to create an account and associate the email address with the user's

organisation so that they can then submit data for the audit / registry / collection that they are assigned to.

Your rights regarding this data:

- Be informed
- Get access to it
- Rectify or change it
- Restrict or stop processing it

If you require information about GDPR and a specific audit / registry / collection, please visit NHS Digital's GDPR Register (https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register).

2.19 Privacy and Cookies

For information on privacy and cookies, please visit NHS Digital's Privacy notice (https://digital.nhs.uk/about-nhs-digital/privacy-and-cookies).