The CAREFUL Platform: privacy impact assessment

CAREFUL Systems Limited

20 November 2020

Contents

Introduction

The CAREFUL Platform

The CAREFUL Platform is a patient-tracking app that runs on mobile or desktop computers through a standard browser. Native iOS and Android apps are planned for later in 2018.

The systems collects and shared patient identifiable data, including demographic details and information about private and sensitive data about the health and disease of individuals.

The system is designed and developed by Careful Systems Limited ('CSL', 'we'). We are committed to the very highest standards of data protection. This document sets out the ways in which we enforce these standards using the principles of 'Privacy by Design' (PbD).

Legal background

Currently, CSL only provides the CAREFUL Platform to users within the UK and so only data relating to patients either temporarily or permanently resident in the UK are stored on the system.

CSL is bound by the UK's Data Protection Act 1998. When considering privacy also takes account of the Mental Capacity Act 2005, the Mental Health Act 1983 as amended by the Mental Health Act of 20007.

We also adhere to the principles set out in the report of the Caldicott Committee in 1997 as amended in 2012. We note in particular — since the CAREFUL Platform intends to assist with this — the seventh principle, namely: the duty to share information can be as important as the duty to protect patient confidentiality

CSL is

- registered with the Information Commissioners Office (ICO)
- certified through the NHS Digital IG Toolkit with Information Governance Certificate of Compliance (IGSoC) Level 2
- a g-Gloud 12 accredited supplier

Security

Preventing access to the data by unauthorised people

What follows is a list of some of the precautions that we have undertaken to ensure that the data on the CAREFUL Platform is inaccessible to unauthorised users:

- All data is stored on a Microsoft Azure server in England, UK. Microsoft is the one of the leading cloud-storage providers in the world and has also been IGSOC Level 2 certified.
- We use an industry standard database storage technology. This database is encrypted transparently at rest. This means that any attacker would not be able to access the data if they had access to the physical storage media.
- Unencrypted access to database functions aside from through the app itself, is permitted only via a small number of specified locations (IP addresses). This means an attacker would have to be physically present in one of our developers' offices to view data or make unauthorised changes.
- All machines in such locations are protected by high-level password protection and suitable local access restrictions.
- The Visual Machine (VM) web-server also uses industry standard technology and is also only accessible using a password known only to CSL and our developers. This password is changed regularly and is a 256-Bit random string.
- All interactions with the web server are through 256-bit HTTPS encrypted channels, so no data can be accessed while in transit.
- No data is stored on users' desktop or mobile device.
- Users are locked-out of the system after a time-out and unable to access data without re-inputing their password.
- User passwords are forced to be 10 characters in length

Our plan is to move within 12 months to a 'native' platform for mobile users. This will allow us to enforce further security measures, such as forcing passcode/face recognition protection, to ensure that data on a mobile device is accessible only by the owner.

Confidentiality

Preventing inappropriate access to data by authorised users

We have spent a great deal of time designing the CAREFUL Platform to balance the need to share data between authorised users while at the same time ensuring that such authorised users do not themselves represent a possible ‘data leak’ and that they do not have access to data they do not need.

The fourth Caldicott principle states that access to patient identifiable information should be on a strict need-to-know basis. We have therefore ensured that there are barriers within the system to prevent unnecessary access by authorised users to data for which there is no clinical need.

We do this by separating users into organisations and then into teams. Users can only see clinical data of patients if they are member both of an organisation, and of a team which is caring for that patient.

Clinical systems are used and managed by teams that have, by their nature, a fluid and changing membership; staff members come and go, temporary staff are hired at short notice. We recognise that it is imperative that such new users can be added quickly to the system. However, we must also control such access.

We have therefore added the following features:

- There are three levels of access: staff users, team administrators and organisational administrators.
- The level of access can only be granted by someone with similar levels of access.
- Only organisational administrators or team administrators can add new users to the system. Team administrators can only add users to their own team.
- All users’ access to the system is time-limited - allowing temporary staff access only when they are on duty.
- All users must provide both a valid email address and a working UK mobile phone number in order to gain access to the system.
- Users are granted access to teams only a team-by-team basis, not to the organisation as a whole. Organisational administrators can access all information within an organisation.

Inter-team transfer restrictions

It is often necessary for good care that patients are moved between teams. Patients may therefore be cared for by different teams at different times. The CAREFUL Platform allows for this by providing a referral and transfer function.

Transfer and referral within the bounds of a single organisation is straightforward, allowing patient data to be shared with more than one team at a time.

However if it also desirable that data is shared between organisations. For instance, care may be transferred between two hospitals or between a hospitals and a community service. To prevent an inadvertent transfer or referral to a 'rogue' or inappropriate organisation, all organisations are verified by CSL before such transfers-out or transfers-in can be undertaken. We recognise that this manual process may cause delay for of the first of such transfers, it ensures that data does not inadvertently 'leak' to unverified or unknown users.

Development Process and development team

We also recognise that 'users' includes the members of staff, developers and sub-contractors to CSL. We have therefore put in place a clear set of processes and procedures to ensure that all members of staff are fully trained in the principles of Information Governance, including the Caldicott Principles. All members of the development staff are aware that sensitive and confidential data must not be accessed unless development or support needs of the users, patients or company demand it.

To make this more likely, we separate the development process and the development environment from real patient data (which we call our 'production environment'). Our development environment is populated with 'fake' patient data in order to allow for testing. There is therefore rarely need for anyone to access data directly within the production environment.

We also ensure that all data access, whether to the development or production environments, is via an Application Programmable Interface (API). This means that data is placed into the database and withdrawn from the database in controlled ways, which are both audited and reportable (see section below).

Reporting and Audit

Ensuring traceability of data

The CAREFUL Platform has been designed with an in-built, robust audit and time-stamp system which records all changes to patient data and to other objects in the system, such as teams and users.

This means that all users can see a clear audit-trail of any changes.

It also allows us to provide to organisations and teams exceptional historical reporting of both patient-data and user-data.

In the unfortunate event of a data breach, this will give us the ability to trace any users involved and to ensure that the extent of any such breach can be accurately assessed.

Data Retention

Our policy is to preserve all patient identifiable data for twenty years in order that any medico-legal queries that may arise can be answered.

Patient-access and control

The General Data Protection Regulation (GDPR)

The GDPR came into force on 25th May 2018. The most significant change from that legislation has been the degree of control and consent that individual patients are allowed over the processing of personal data, and over who has access to this data.

As well as being able to provide a complete description of the data held currently about a patient, the CAREFUL platform can also provide an audit log of all previously stored data and changes. Logs of team activity also allow patients to be informed, should they wish to be, about who and when their data was accessed.

CAREFUL patient facing app

Our plan is also to provide a Patient App which will provide a level of oversight and control for individuals whose data is held by the CAREFUL Platform. Using the Patient App, users will be able to:

- See all data that has been recorded against them
- See who has accessed their record and when.
- Contribute or comment on data in their record.
- Control and determine which individuals, teams and organisations have access to their data
- Add and manage other users — such as family members — who can then view the patient's record

In order to make patient access viable, it will be necessary to reliably identify and validate any individual seeking to gain access to the system. We will base this on industry standard practices, such as those used to open or manage a bank-account online.

Our intention is to make this app available by the middle of 2021.

Please direct any questions concerning privacy to privacy@careful.online