west midlands
ACADEMIC HEALTH SCIENCE NETWORK

Heartflow Data Protection Impact Assessment Guidance

Improving health and creating wealth

Office 12 > Ground Floor > Institute of Translational Medicine > Heritage Building
(Queen Elizabeth Hospital) > Mindelsohn Way > Edgbaston > Birmingham > B15 2TH
+44 (0)121 371 8061 > info@wmahsn.org > www.wmahsn.org > @wmahsn

Overview

Purpose

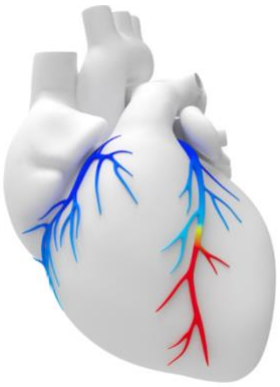
This document provides guidance on the Heartflow product to inform a data protection impact assessment. It should be used to support the implementation of the product in NHS Trusts. The impact assessment has been prepared by the West Midlands Academic Health Science Network (WMAHSN) to support Trust Information Governance leads.

The West Midlands Academic Health Science Network leads, catalyses and drives co-operation, collaboration and productivity between academia, industry, health and care providers and commissioners, and citizens, and accelerates the adoption of innovation to generate continuous improvement in the region's health and wealth. It operates under licence from NHS England.

The data protection roles are as follows:

- Data Controller- NHS Trust
- Data Processor - Heartflow UK Ltd (Company number 10018961)

Background



HeartFlow FFR CT is a coronary physiologic simulation software for the clinical quantitative and qualitative analysis of previously acquired Computed Tomography (CT) DICOM data for clinically stable symptomatic patients with coronary artery disease. Evidence shows a 61%[1] reduction in patients required invasive angiogram with no detriment to outcomes. This produces a 26%[2] reduction in treatment cost.

Using data from a standard CT scan, the non-invasive HeartFlow Analysis creates a personalized 3D model of the coronary arteries and analyzes the impact that narrowing of the arteries have on blood flow. It is suitable for Clinically stable symptomatic patients with suspected coronary heart disease.

The use of Heartflow is supported by NHS England and has been clinically endorsed by NICE through the Medical technologies guidance (MTG32) and supports the NICE Clinical guideline (CG95). The Heartflow product is classified as a class IIa medical device.

1 Douglas et al. Clinical outcomes of fractional flow reserve by computed tomographic angiography-guided diagnostic strategies vs. usual care in patients with suspected coronary artery disease: the prospective longitudinal trial of FFR CT: outcome and resource impacts study. Eur Heart J. 2015;36(47):3359-67.

2 Data on file. In the PLATFORM Trial, the mean one-year per-patient cost for the usual care strategy was $12,145 compared to the $8,127 cost for the HeartFlow-guided strategy, a cost reduction of 33 percent. Not reported in the study results, mean costs remained 26 percent lower among the HeartFlow-guided patients than among usual care patients ($9,036 vs. $12,145, p <0.0001) when factoring in the $1,500 cost of the HeartFlow Analysis.

Summary of Compliance

Principles	Assessment of Compliance
Principle 1 – Lawfulness, fairness and transparency	There is a legal basis for the processing of account information, CT images & analysis and support tickets. Article 9 (2) (h) provides a legal basis when processing is necessary for the purposes of preventive or occupational medicine
Principle 2 – Purpose limitation	Processing is limited to the stated purpose - providing a personalized 3D model of the coronary arteries and analyses the impact that blockages have on blood flow
Principle 3 – Data minimisation	Account information and support tickets consist of the minimum staff data to use the system. This is personal identifiable data. CT images and analysis are anonymised and so do not constitute personal identifiable data.
Principle 4 – Accuracy	User data is to be maintained by the Trust through the portal. Issues with CT images and analysis are addressed through the Heartflow support function.
Principle 5 – Storage limitation	Identifiable data is retained by Heartflow for 7 years. De-identified data is used to improve the Heartflow product and so may be retained for longer.
Principle 6 – Integrity and confidentiality (security)	Heartflow complies with organisational (ISO 27001, HIPAA) and technical standards. It relies upon the Amazon S3 cloud that also complies with these standards. Use of the S3 cloud is permitted by NHS policy (amended January 2018).
Principle 7 – Accountability	Compliance with the principles is enforced through a contract between NHS England and Heartflow. The Trust becomes a party to the contract when it signs the ITP.

Further Information

www.heartflow.com

Processing Overview

Summary

Category	Who's Information	System	Where is it going?	Nature and Purpose of Processing	Frequency	Method of Transport	PID/No PID	Type of Information
Account information	Controller staff (clinicians / IT)	Heartflow	Stored within Processor's Amazon S3 UK instance	Permits users to login to portal and receive email updates	Real-time	HTTPS	PID	Business identifiers - email address, - telephone number - organisation First Name Last Name
CT Images & analysis	Patients undergoing CT scans	CT / PACS -> Heartflow	Stored in Connect virtual appliance by Controller and in Processor's Amazon S3 UK instance. The de-identified CT DICOM data is stored in the Amazon S3 US instance	Required for medical analysis and reporting	Real-time per CT scan	TLS 1.2	PID	CT scans (DICOM images)
Support Tickets	Controller staff	Heartflow Ltd support system		Management and resolution of support issues	Real-time	Email Phone call	PID	Business identifiers Support information and associated metadata

Data Categories

The Heartflow system contains:

- **Account Information** (name, email address, organisation) - to permit Trust staff to login to the Heartflow portal and view and/or administer the analysis.
- **CT images & analysis** – CT images and the associated analysis that forms the core of the Heartflow product.

Heartflow Ltd maintains the following information for the purposes of providing the Heartflow service:

- **Support tickets** – for the tracking, management and resolution of support issues in relation to the Heartflow product.

Justification

Data Category	PID	Justification
Account Information		
Name	X	Staff data - Required for the administration of the service
Email Address	X	Staff data - Required for the administration of the service
CT images & analysis		
CT Images	X	Patient data - Images necessary for the purpose of the tool
Analysis	X	Analysis necessary for the purpose of the tool
Results	X	Results necessary for the purpose of the tool
Support tickets		
Heartflow to complete	X	Staff data - Required to support product

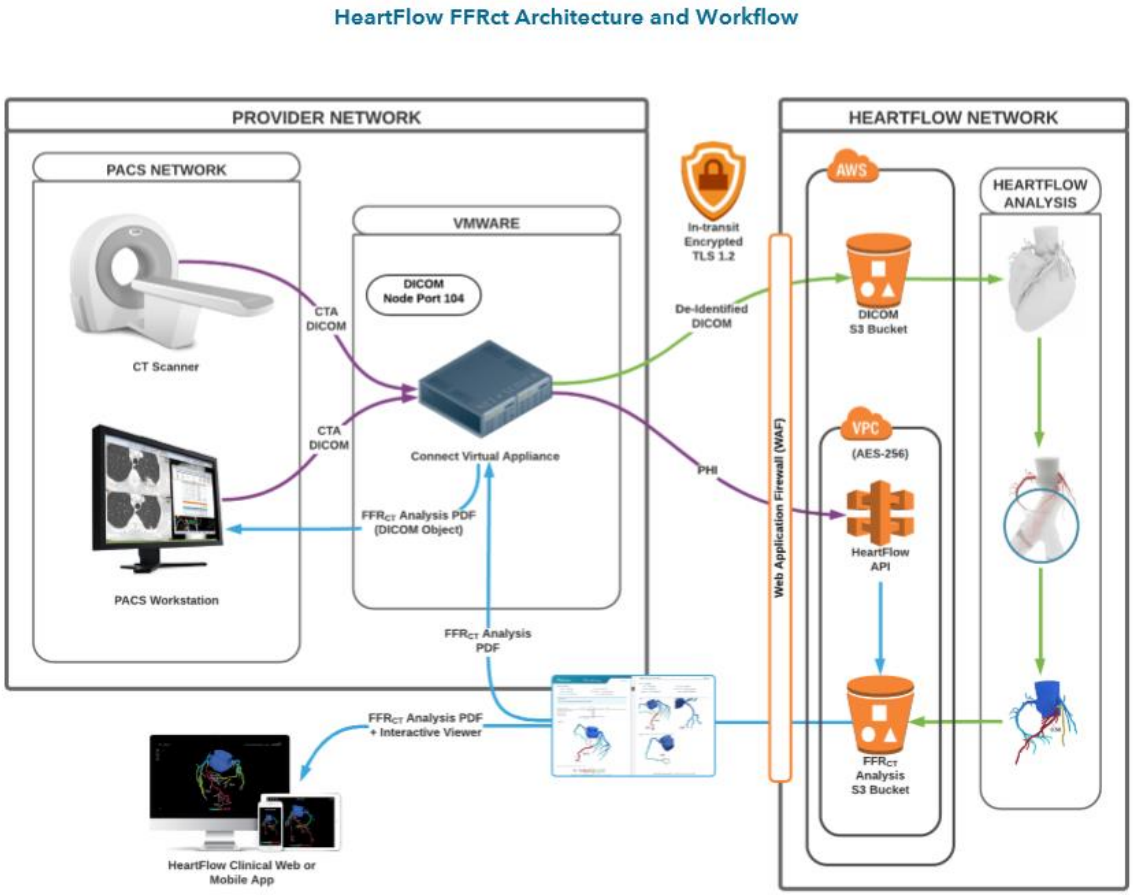
Data Flows

Account Administration

The Heartflow portal requires users to authenticate to it using email address and password. Once authenticated to the portal users can see the status of CT image submissions, change their password and (if authorised to do so) administer user accounts for their organisation.

The initial user is created by Heartflow. Subsequent account maintenance is the responsibility of the Data Controller.

CT Images & Analysis



1. CT images are capturing using a CT scanner and transmitted to the HeartFlow Connect virtual appliance, operating within the Trust's IT. This transmission can either be directly from the CT scanner or via the PACS system.
2. HeartFlow Connect transmits the PID over the Internet to the Heartflow network contained with the Amazon S3 UK instance.
3. De-identified CT DICOM data is then sent to the USA Amazon S3 instance.
4. The Heartflow network performs the analysis and creates a report. This involves Heartflow staff refining the image and then computer analysis. The USA only has access to de-identified data.
5. Users registered with Heartflow are notified the HeartFlow Analysis is available via email. No personal information relating to the patient is transmitted in the email.
6. Registered users can view and download the HeartFlow Analysis. The Analysis is delivered to the hospital PACS. Users can also view a 3D model online however this is only visible via the Heartflow Clinical Web App and Mobile App.

Support Tickets

1. User logs support call.
2. Support call is managed by US support team.

Data Protection Impact Assessment

Stakeholder Consultation

Heartflow was developed and first licenced in the USA. In the UK, Heartflow is endorsed by NICE and recommended by NHS England. The tool is in use across the country.

Legal Basis for Processing of Personal Data

Article 9 (2) (h) provides the legal basis for the processing of the patient's medical information (including the CT scan and the Heartflow results) by the Trust. Heartflow does not use personal data as it is de-identified.

> *Article 9 (2) (h) – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*

Article 6 (b) provides the basis for the processing of **Account Information** and **Support Tickets**)

> *Article 6 "Lawfulness of processing" - 1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> *…(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

Data Retention Period

Data Category	Retention Period
Account Information	7 years post account de-activation
CT images & analysis	7 years (PID) De-identified images can be retained longer to train the recognition model
Support tickets	7 years

Note that the final report should be placed in the patient record (it is available as a PDF so this can be electronic) and retained as per Trust standards.

Data Quality Standards

Account information can be edited by the Data Controller to ensure it remains up to date. Errors with CT images and analysis should be reported to Heartflow for resolution.

Images that cannot be processed by Heartflow are rejected and the Trust informed.

Individual Rights

Right	Assessment of Compliance
1. The right to be informed	A patient leaflet is published on the Heartflow website. NHS Trusts should inform patients of the processing of clinical information on a wider basis.
2. The right of access	The PDF report will form part of the patient's medical record independent of Heartflow. Rights to access should be managed in accordance with the Trust's subject access request policy.
3. The right to rectification	Patients can exercise their rights in this area as per Trust standards
4. The right to erasure	Reports should be retained in the patient's medical record in accordance with Trust policy.
5. The right to restrict processing	Patients can elect not to undertake a Heartflow test as part of their normal rights to consent or dissent to treatment.
6. The right to data portability	The analysis is provided in a PDF format for data portability. The interactive viewer information is not portable.
7. The right to object	Patients can elect not to undertake a Heartflow test as part of their normal rights to consent or dissent to treatment.
8. Rights in relation to automated decision making and profiling.	Heartflow arguably constitutes profiling however the results are not an automatic decision. They are to support the decision of a suitably qualified clinician.

Cyber Security Technical and Organisational Controls

Organisational Controls

A GDPR compliant contract exists between NHS England and Heartflow Ltd. The Trust is a party to this contact.

Patient Personal Identifiable Data is retained within the UK. De-identified patient data, staff data and support information are retained within the USA.

Heartflow is accredited as follows:

Accreditation	Certificate Number
ISO/IEC 27001:2013	IS 670475
HIPAA Compliant	

HiTrust Common Security Framework (CSF)	
ISO13485 Medical Devices Quality System	

Technical Controls

The security controls are described in the Heartflow document FFRCT v2.x Security Overview available on request. To note only authorised users with a login can access the Heartflow system. Administration of user accounts is maintained by the Trust.

Heartflow uses the Amazon S3 cloud. NHS policy on cloud was updated in January 2018. NHS and Social care providers may use cloud computing services for NHS data. Data must only be hosted within the UK - European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.

Amazon Web Services (AWS) management has a strategic business plan and information security program that includes risk identification and the implementation of controls to mitigate or manage security risks (see AWS Risk and Compliance Whitepaper).

AWS Cloud infrastructure meets the requirements of an extensive list of global security standards, including but not limited to: HIPAA, ISO 27001, SOC, the PCI Data Security Standard, FedRAMP, Japan's CS Mark & My Number Act, Australian Signals Directorate (ASD) Information Security Manual, and the Singapore Multi-Tier Cloud Security Standard (MTCS SS 584).

Heartflow is registered with the Data Protection Toolkit.

Risk Assessment & Further Actions

Source of Risk and Nature of Potential Impact	Mitigation	Likelihood of Harm (Remote, possible or probable)	Severity of Harm (Minimal, significant or severe)	Overall risk (Low, medium or high)
Cyber security breach	Maintenance of organisation cyber security controls (ISO 27001:2013) Register with and respond to CareCERT alerts	Possible	Significant – loss of service / loss of staff account information	Medium
Patients unaware of Data Protection rights	Provide published patient material (complete)	Possible	Minimal	Low
Loss of data as Trust does not store report in medical record and Heartflow deletes data at end of retention period	Ensure report is stored within patient's record.	Possible	Significant	Medium