DATA PROTECTION IMPACT ASSESSMENT

Centric Health Coronavirus Programme

Remote Monitoring application

NAME OF CONTROLLER: Centric Health

NAME OF PROCESSOR : Luscii Vital

What are the objectives of this methodology?

By following this process we will:

1. Ensure compliance with applicable legal, regulatory, and policy requirements for privacy.
2. Determine the risks, including to individuals, in terms of damage and distress caused when personal data is mishandled, and organisational risks, such as financial and reputational damage resulting from data breaches.
3. Evaluate protections and alternative processes to mitigate potential privacy risks.
4. Identify actions to be taken to reduce privacy and information security risks.
5. Embed privacy by design and other appropriate information security measures into the specification, design and build of systems and procedures.

The outcome of a properly conducted data protection and information risk assessment should be reduction in privacy, security and reputation risk, improved compliance with data protection legislation, improved systems and greater trust among data subjects and other stakeholders.

Centric Health & Luscii Vital can rely on a DPIA to provide evidence in demonstrating compliance in two key areas:

1. Were all material risks identified? An organisation can only comply with data protection requirements if it has identified and addressed the risks that arise in connection with its processing activities.

2. What appropriate steps were taken to address those risks? The DPIA provides a record of the steps that were taken to resolve or mitigate any danger to the rights and freedoms of data subjects.

The DPIA should examine safeguards to lower any identified risk by the DPIA, Recital 90 of the GDPR states “That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation”

Codes of conduct are also mentioned in Recital 98 as a mechanism to calibrate controllers and processors.

Recital 76 covers risk assessment

“The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.”

Recital 77 goes on to state that risk guidelines can be from certifications, codes of conduct and that the European Data Protection Board will also give guidelines

Data Protection by Design and by Default

Article 25 of the GDPR addresses certification mechanisms as a means to keep data safe and secure alongside the controller or processor taking the appropriate technical and organisational measures to safeguard personal data.

Q1: Will the project involve the processing of personal information? **Y** N If YES please give details (i.e. whose and what categories of personal data (e.g. name, dates of birth etc etc.)). Processing includes storing data as well as collecting, accessing, updating, sharing, destroying etc.	
Category of Personal Data	**Purpose of Processing**
Administrative: name, address, contact details (phone, mobile, email), dates of appointment	Necessary to support the administra practice
Medical Records: Individual Health identifier, GMS number, PPSN, date of birth, gender, family members, family history, contact details of next of kin, contact details of carers, vaccination details, medication details, allergy details, current and past medical and surgical history, genetic data, laboratory test results, , and other data required to provide medical care.	Necessary to provide patient care i
	The PPS number is needed for spe certification

Security of Processing

Article 32 of the GDPR covers Technical and Organisational measures to safeguard personal data in line with the risk and suggests using encryption and pseudonymisation of personal data, it highlights the importance of confidentiality, integrity, availability and resilience of processing systems and services. Article 32 also covers the ability to restore data in the event of a loss of data and a process for testing the technical and organisational measures around the processing. Appropriate levels of security must be undertaken in accordance with the data processing taking place.

First section will be answered by Centric Health

Second section will be answered by Luscii Vitals

Luscii Vitals			
Personal Data	**User**	**Required?**	**Storage**
First Name	Patient, Provider, Admin	Required	2 years after termination of the account
Last name	Patient, Provider, Admin	Required	2 years after termination of the account
Gender	Patient	Required	2 years after termination of the account
Address	Patient	Optional	2 years after termination of the account
Street	Patient	Optional	2 years after termination of the account
House number	Patient	Optional	2 years after termination of the account
Addition	Patient	Optional	2 years after termination of the account
Location indication	Patient	Optional	2 years after termination of the account
Postal Code	Patient	Optional	2 years after termination of the account
Place	Patient	Optional	2 years after termination of the account
Country	Patient	Optional	2 years after termination of the account
Date of birth	Patient	Required	2 years after termination of the account
Email	Patient, Provider, Admin	Required	2 years after termination of the account
Phone	Patient	Required	2 years after termination of the account
Healthcare organization	Patient, Provider, Admin	Required	2 years after termination of the account
User name	Patient, Provider, Admin	Required	2 years after termination of the account
Type user	Patient, Provider, Admin	Required	2 years after termination of the account

Profile picture	Patient, Provider, Admin	Optional	2 years after termination of the account
Group	Patient, Provider, Admin	Optional	2 years after termination of the account
Program	Patient	Required	2 years after termination of the account
Notes on measurement	Patient	Optional	2 years after termination of the account
Measurements	Patient	Required	2 years after termination of the account
Frequency measurements	Patient	Required	2 years after termination of the account
Threshold values	Patient	Required	2 years after termination of the account
Alerts	Patient	Required	2 years after termination of the account
Language	Patient, Provider, Admin	Required	2 years after termination of the account
Time zone	Patient, Provider, Admin	Required	2 years after termination of the account
Patient number	Patient	Optional	2 years after termination of the account
Patient absence dates	Patient	Optional	2 years after termination of the account
User actions (login, logout etc)	Patient, Provider, Admin	Required	2 years after termination of the account
IP addresses	Patient, Provider, Admin	Required	2 years after termination of the account
Call history	Patient, Provider, Admin	Required	2 years after termination of the account
Push notification ID	Patient	Optional	2 years after termination of the account
iOS / Android device version	Patient	Required	2 years after termination of the account
Browser version	Patient, Provider, Admin	Optional	2 years after termination of the account
App version	Patient, Provider, Admin	Required	2 years after termination of the account

Notes on the Legal Basis for Processing of Data

It is not possible to undertake medical care without collecting and processing personal data and data concerning health. In fact, to do so would be in breach of the Medical Council's 'Guide to Professional Conduct and Ethics for Doctors'. The legal basis for processing of data by GPs is provided by the following articles in GDPR: Article 6.1(c), 6.1(d), 6.1(e) and Article 9.2(h) and 9.2(i).

Article 6.1(c) in relation to the lawfulness of processing states: 'processing is necessary for compliance with a legal obligation', for example reimbursement claims.

Article 6.1(d) in relation to the lawfulness of processing, states: 'processing is necessary in order to protect the vital interests of the data subject or of another natural person'.

Article 6.1(e): in relation to the lawfulness of processing, states: 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. This includes the use of PPS numbers by GPs.

Article 9.2(h) in relation to the processing of special categories of personal data, states: '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'; Paragraph 3 relates to the processing of data concerning health by medical practitioners subject to professional confidentiality under the regulation of the Irish Medical Council.

Article 9.2(i) relates to processing necessary for reasons of public health.

Article 6 and Article 9 need to work in conjunction with one another. So for instance a GP will rely upon a combination of Article 6 to process non sensitive data and Article 9 conditions to process special categories of data.
The processing of personal data in general practice is necessary in order to protect the vital interests of the patient and for the provision of health care and public health. The lawfulness of processing data for the provision of medical care in general practice is not based on consent.

However, **explicit and informed consent** is required for some defined data outflows. This will be requited for patients to avail of this service with Luscii Vital. **Categories of Recipients Whom We Share Personal Data**

<u>Categories of Recipients Whom We Share Personal Data</u>

These are broken down into four categories as shown in the table below: sharing data in relation to the provision of medical care, sharing data with data processors where a contract is required, sharing data under legal arrangements, and sharing data for public health purposes.

Categories of Recipient	**Description**
Health and Social Care Providers	Other GPs, Health Service Executive, Voluntary Hospitals, Private Hospitals and Clinics, Private Consultants, Out of Hours Services, Pharmacies, Nursing Homes, Hospital Laboratories, Practice Support Staff, GP Locums and other health care providers
Data Processors, with a contract	***Luscii Vital***
Legal Arrangements	Coroner, Revenue, Social Protection, Medical Council

Public Health	Infectious disease notifications

Q2: Will the project involve the use of an external contractor or supplier (i.e. not a member of the Luscii Vitals group) to process personal data or other confidential information? This includes hosting or maintaining IT systems and applications.
Luscii Vitals
Luscii Vitals • Amac for the logistics of Ipads, if we are providing you with Ipads (In the Netherlands only) • AWS for data hosting • Branch.io for your onboarding • Centraal Boekhuis for the logistics of measurement devices. (if we are providing you with measurement devices) • Student aan Huis for installation services (In the Netherlands only) • Zendesk and Intercom for customer support • Mandrill / Mailchimp for sending email and managing email lists • Vidyo for video chat • Google Analytics for user behavior analysis • Crashlytics/Fabric/Sentry for monitoring crashes of the smartphone apps All third parties are reviewed and approved by our compliance team before being contracted. Where applicable, we have data processing agreements in place.

Q3: Will the project involve transfers of personal data outside EEA , to a third country or US .
Centric Health note the Netherlands are in EEA therefore GDPR and national laws apply**.**
Luscii Vitals – Not applicable.

Q4 : Will the project involve processing special categories of personal data?

Centric Health are aware of its responsibilities under Article 9 GDPR
https://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm

Centric Health will require explicit consent from patients article 9 2(a) – (a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes,

Adoption and understanding of Article 9 GDPR with legal basis of consent. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

Centric Health received a complete DPIA from Luscii. Details can be issued under the approval of Luscii.

Q6 : Will the project involve processing other high risk personal data?

There is no definition given on what exactly constitutes high risk under the GDPR, only that it should be able to be determined following assessment. Processing of large amounts of data or sensitive data are given as examples that are likely to result in high risk in the law.

Centric Health acknowledge the following high-risk personal data includes the following:

- Personal information relating to some vulnerable adults
- Any other personal information that would cause damage or distress to individuals if disclosed without their consent

In the relationship there is the use of innovative technologies & Tracking

Luscii Vitals –
Centric Health received a complete DPIA from Luscii. Details can be issued under the approval of Luscii.

Q6 : Will the project compel individuals to provide personal information about themselves?

- Yes , this will be done under explicit consent from Centric Health Patient . See Q1.

Online form will be agreed and tested by core group from Centric Health. All online forms will ensure ease of understand for patients. Consideration will be made that patients may be in a heightened level of stress or anxiety, the may not be comfortable with IT apps.

Details will be provided to patient giving clear instructions, FAO, links to Luscii , links to privacy policy for Centric Health and Luscii , contact e-mail for Centric Health and Luscii .

Legal basis for Centric Health and Luscii - performance of a contract between Luscii and customer (healthcare provider

Luscii Vitals – privacy policy -

https://luscii.com/privacy-policy/

Q7 : Are you using information about individuals for a purpose it is not currently used for, or in a way not currently used?

Centric Health is responding to a public health crisis. Data collected is for the purposes of managing actual, suspected or potential cases of COVID-19.

Q8 : Does the project involve you using technology which might be perceived as being privacy intrusive (e.g. the use of biometrics or facial recognition)?

No - This will largely be led by Centric Health GP. The GP will have spoken to the patient . There is no use of biometrics or facial recognition

Luscii Vitals – No

Q9 : Will the project require you to contact individuals in ways that they may find intrusive

No – all calls to Centric Health will be pre-arranged and will be noted in how this technology will work . Patients will be engaging daily through the App. Calls from the clinical team will be triggered by patient entered data that could indicate a clinical concern or if a patient requests a call back from the clinical team through the app. This is not an emergency service and patients will be made aware that they will receive a call back within 24 hours.

Luscii Vitals – No patients will liaise with their Centric Health Practice. Luscii will act as support in case of system issues . All system issues will be referred to support@luscii.com.

INFORMATION RISK MANAGEMENT CHECKLIST

Describe the information flows and security controls

Why will the information be collected/used?

As there is a current global pandemic with rapidly escalating numbers of cases in Ireland and Europe, a rapid response is required in to the developing scenario. Centric Health has identified the need for a solution to support the community management of patients with milder disease. In particular, such a system needs to support safe self-management, limit unnecessary contact with health care professionals and hospital system, and embed (and improve) automated triggers to identify early markers of deterioration and rapid notification to clinicians.

A cloud based Remote Patient Monitoring (RPM) software solution allows remote diagnosis, assessment and monitoring of patients with COVID-19 or suspected COVID-19 or at-risk of COVID-19 infection, supported by a virtual clinic of GPs delivering teleconsultations to patients.

Patients enter the solution via a form embedded in our website They are subsequently approved or declined by the team for entry based on safe coverage of volumes. Patients on the system enter symptoms on a daily basis. That information is immediately available for review on the clinician end of the software, alerts are automatically triggered if outside of a clinically acceptable range. In such a case, clinical intervention is warranted and the case is passed to a GP. Should a patient deteriorate, warranting review at a healthcare facility, a referral document is prepared as per standard practice.

Security Controls - Luscii

Policy

This document is the information security policy:
https://www.notion.so/luscii/Information-Security-Policy-65f8f402114248d4a19f53ec6ca9df09

Encryption

FileVault is used on all macbooks, this encrypts the entire disk

Anonymisation

The Luscii vitals API database on acceptance is an anonymized copy of production for the following reasons:

- It allows testing with production-like data to assess the looks and performance impact of a new release.
- It allows limited testing of a data migration with production-like data before actually applying it on production
- It provides the possibility of fine-grained authorization for developers, following the principle of least privilege, even though we might not do that at the moment

Traceability (logging)

All logs generated by the application or infrastructure is centralized into a Fluentd service, and from there sent out again to multiple targets.

Containers that are part of the Connect Docker environment send their logs directly to Fluentd. Other systems can use the Connect Log HTTP endpoints to provide their log data.

From Fluentd all logs are sent to ElasticSearch. The data in ElasticSearch is protected as strongly as our other data, notably it cannot simply be altered or erased by an attacker without administrative access. Using conventional access methods only allows you to append new log entries.

The log data in ElasticSearch is made searchable via the Kibana interface. This allows for log analysis during development, after an incident, or simply to visualize trends in the warning and error behaviour of our products. In the Product tactical meeting we look at these trends and discuss any abnormalities.

The application generating the log data decides on identifiers to incorporate into the log. For example a session identifier can be added to all log entries related to that session can be correlated. Besides this we use common identifiers such as (internal) user id and unique request id. It's good practice to assign as many identifiers as are available for the best possible correlation.

Log entries are generally divided into four levels of severity:

Error: in the case of a failure that breaks user functionality. This typically requires a code or configuration fix.
Warning: in the case of validation errors for user input. The user should be presented with an instruction on how to correct the input and try again. Warning also covers non-critical failures, e.g. if a retry will be scheduled automatically that tries the operation at a later point in time.
Info: notable messages that help in diagnosing issues. Operation success messages are typically useful so that their absence can indicate a problem.
Debug: messages that include detailed information which may be privacy sensitive. This is useful for application developers reproducing a problem and is always turned off on production for privacy reasons
On all Luscii systems the clocks are synchronized with public time servers using NTP. This ensures that log entries are correctly ordered. Whenever the log entry is generated from a client device (e.g. an iOS device) where the time may be different, the log is routed via the Connect Log HTTP endpoint so that a server time is used. This ensures that changing the device system clock does not hide log entries

Clamping down on malicious software

Standard antivirus software in macOS

At Luscii all workstations are a Macbook, equipped with macOS. If you switch from a Windows laptop to a Mac, you may be inclined to install an antivirus program. Many users do not know that macOS has a security program as standard.

There are standard programs on the mac that protect you against malware and are switched on by default. What is important is that the most recent updates are always installed from macOS.

How does antivirus work on the Mac?

The standard tools that are present in macOS:

- XProtect (a list of malware definitions)
- File Quarantine (checks whether the software appears in the list of malware definitions)
- Gatekeeper (prevents you from simply installing software from unknown parties)

More information about Apple security: [https://www.apple.com/macos/security/ ---------- (https://www.apple.com/macos/security/)

Layered security:

As standard, macOS offers protection against malware. Traditionally, the Mac doesn't suffer much from malware. Yet the best security is a layered security. At Luscii the following layers of security are against malware:

G Suite (Google Mail, Google Drive) - Enhance phishing and malware protection
macOS - standard Apple security (XProtect, File Quarnatine, Gatekeeper)

Kolide - monitor security updates for mac devices and search for evidence infection from known / common malware variants.

Backups
Classified as follows:
Product Infrastructure
Product data
Non-product data

Product infrastructure

Infrastructure is the provisioning and configuration of servers and network components that comprise the foundation for our product to run on. Since we maintain this ourselves, we also need to have appropriate backup in place.

Rather than backing up the current state of infrastructure, we make use of Infrastructure as Code. This is a way of working rather than a specific technique. It has several advantages:

- A backup is inherent, since all infrastructure is managed by
- code, and the code is stored in GitHub Changes are automatically part of the development and review process
- Any configuration drift can be detected and rectified by periodically applying the infrastructure as code playbooks

- In case of catastrophe, the infrastructure as code playbooks can be executed again and the infrastructure entirely built from scratch

The tool we use for this is Ansible. Infrastructure is expressed in Ansible Playbooks which can be found here:
https://github.com/Luscii/connect-ansible

All infrastructure is stateless, meaning it doesn't contain any data worth backing up. For actual data, see next section.

Product data
All product data is stored in managed AWS databases. These are set up in such a way that:

- They are redundant, so a slave node is already a live backup of a master node
- Full snapshot backups are made every day
- Transaction log backups are made every 5 minutes
- Backups cannot be deleted manually, only via expiry of the backup retention window
- Backup retention is 30 days

This means that in an event where we lose both master and slave nodes, we can always restore the database again from a snapshot. We can choose any point in time with a precision of 5 minutes, meaning at most 5 minutes of data is lost.

When a snapshot is restored (meaning: a database instance is created from a snapshot) we set the identifier of the original database instance. The effect is that the URL stays the same, so any software components connecting to that database will be able to work again without reconfiguring them.

The procedure for disaster recovery, as detailed below, is periodically tested on the acceptance environment. The testing schedule can be found in the . Whenever a test is performed, this is also documented there. The role accountable for performing disaster recovery testing is D evOps.

Test data

Luscii at the moment has two environments on which we test our upcoming features and releases, the data on the test environment is not related to any real user and can't be accessed without a username and password. Our databases can only be accessed by select users from our development team and can only be accessed on the network of our Amsterdam office, VPN access is available for specific users from our team but is protected by firewall, this ensures the ability to revoke access per user to this data at all times.

For our Acceptance environment we use a copy of the user data from our production environment, but only after going through steps to ensure that the data can't be traced back to any person, this means that the user information is changed with the help of scripts into data that is untraceable to any real user of our solutions, specifically we change all contact information meaning: name, address, email-address, birthdate, patient-number and UMO-Code.

We do not change measurement data as we use it to test and improve the experience of our users, this data is not traceable to any user after the aforementioned changes are done.

Backup restore procedure

Procedure for a full backup restore from snapshot:

- Identify database instance to be restored
- Identify desired snapshot and optionally a desired point in time Prepare logging dashboard with warnings and errors
- Make a note of the database identifier and its other settings

- Shut down the application
- Create a new instance from the snapshot, using the same settings as the original instance. Use a temporary name
- Important: Not all configuration is automatically copied from the original. Notably the security groups will have to be set manually.
- Deactivate current database:

When practicing on acceptance: destroy the current instance
When practicing on production: rename the current instance (this will already cause connection failures) When not practicing: rename the current instance if it still exists

- Create a new instance from the snapshot, using the same settings as the original instance
- Rename the restored database to that of the original database
- Bring the application back up
- Monitor the logging dashboard for a decrease in warnings and errors
- Follow up:

When practicing, check off the planned item in the Compliance Calendar, or create a new item (from template) if it was unplanned
When not practicing, follow the Incident Process to inform customers etc.:
Incident process

Non-product data
Any data not generated by our product (examples are Google Drive contents, invoicing, signed contracts, …) are hosted in cloud services which maintain their own backups

Network security
All network related services are managed by iUnxi. This includes the following services:

- Local Area Network
- Wireless Network
- Firewall cluster
- Connectivity
- Infrastructure Management Managed Wireless Network
- Remote Access VPN

All documentation and service level agreements are stored in google drive

Endpoint Protection
All workplaces are defined within Kolide. It scans all workplaces on the following best practises for security:

- Find my Mac enabled
- System Firewall enabled
- Auto update enabled
- FileVault enabled
- Remote Login disabled
- Gatekeeper enabled
- SIP configured

Besides this it also comes with alerts for many useful security risks. Some examples are:

- Plaintext 2FA recovery codes
- Unencrypted SSH keys
- Evil browser extensions
- Malware Cryptocurrency miners

Email Protection

Gmail is the standard email service used at Luscii. How is Gmail secure?

1. Antivirus scanner
2. Advanced phishing and malware protection for incoming email
    1. Place emails into a quarantine
    2. Protect against anomalous attachment types in emails
    3. Protect your Google Groups from inbound emails spoofing your domain
3. All traffic use HTTPS
4. 2 Factor Authentication
5. Brute Force Attack protection
6. End-to-end encryption to secure email and attachments using chrome extension Flowscript

Read Google Cloud Security and Compliance whitepaper

Encryption

FileVault is used on all MacBooks, this encrypts the entire disk.

Luscii does not use any cryptography with legal implications. In other words; we use publicly available (open source) ciphers and we do not have any restrictions on the key sizes.

Malware Protection

All workplaces are installed with Bitdefender GravityZone endpoint protection against malware.

Also all workplaces use the default Mac OS protection against malware XProtect (a list of malware definitions), File Quarantine (check if software is listed in the dictionary of malware) and Gatekeeper (prevents to install software from unknown vendors).

Physical access control

Management/administration

The alarm codes and access tags (authorization) are the responsibility of the Gatekeeper. He / she has as one of the facility tasks, the issuing / taking of alarm codes, tags and keys for access to the Luscii building in Amsterdam. The assignment for issuing / collecting is triggered by the recruitment process. The on- or off-boarding checklist specifies whether the associated employee will receive or hand in an access tag, alarm code and key. The issue is recorded in the list The Gatekeeper's Administration, which is managed by the Gatekeeper.

The employee signs a loan agreement when a key, tag and / or alarm code is issued. The loan agreement also describes how the employee should deal with the tag and / or alarm code. The closing procedure is also described herein.

Alarm system

The alarm system in Amsterdam has 2 zones: Spuistraat 112-A and Spuistraat 114-A. All employees have a personal code with which they can activate / deactivate the alarm. ATC carries out the follow-up of the alarm.

Physical access

Access control starts with access to the front door and can only go through electronic access security or **with a physical key. Both the central access and the access to the office space (2 zones) take place via electronical access.**

Electronic Access to the front door of office building in Amsterdam is regulated via the Bekey app. The employee can open the door via the Bekey app, after which the lock is activated to open the door. The authorization is arranged via a management platform.
There is always a key as Back-up present, The Gatekeeper's Administration states who is in possession of this key.

In addition, every office wing (zone) of Luscii is protected with an electronic access protection. Every Luscii employee has a FOB key with a unique number which is registered per employee to gain access to each office wing.

Guests

The front and office door is not freely accessible, the visitor must always ring the bell. The Luscii employee who opens the door will ensure that the visitor arrives at the right employee. If the visitor does not want to use the elevator, the stairs to the first floor can be taken.

Security measures

Cleandesk policy with Digital working At Luscii a paperless office is stated.

Destruction of papers Within the office space of Luscii, there is a separate container/bin to confidentially destroy sensitive information on paper.

Closing round The closing round takes place every evening by the last

employee to leave the office. During the closing round, attention is paid to

the following:

1. open windows and doors;
2. switch off air-conditioning;
3. equipment that is still on (such as water heaters and toasters);
4. blocked emergency exits;
5. lighting;
6. persons left behind (in the toilets).

If there are no more people on the first floor, the alarm for the first floor zone is triggered next to the entry door of each zone.

Special areas with extra security

Patch cabinet, for general patching of cables (ethernet and telephony) on the entire floor (2 zones). This also includes the switches and routers. The patch cabinet is closed and is situated in the closet (which can be closed) next to the entry door within the office on the first floor (Spuistraat 114-A). The cabinet is only accessible to the Gatekeeper. When access is needed the employee needs to ask permission to the Gatekeeper.

What information will be processed? This means types of data (e.g. name, date of birth, telephone number), specifying any special categories of personal data and any other high risk personal data including financial or location data. - **AS ABOVE**
What number of individuals will have their data processed (approximately)? Unknown Number will be monitored. Centric Health has approximately 400k patients.
How will the information be obtained? Centric Health patients will log onto https://www.centricgp.ie/ and choose their own practice website. The practice homepage will have a link the patient may click to apply for the Centric Health Coronovirus Programme. If the programme is extended to include patients not currently registered with Centric Health, they will access this programme via https://www.centricgp.ie/centric-medical/ Privacy policy of both Centric Health & Luscii . Consent requirement and details. Opt our link or e-mail support@luscii.com.
Describe the security controls to be applied to the process of collection? Luscii https://www.notion.so/luscii/Information-Security-Policy- 65f8f402114248d4a19f53ec6ca9df09
How will the information be destroyed (e.g. secure erasure)? Centric Health will only retain data necessary to carry out the function. Full rights of the data subject will be adhered to in line with GDPR. Luscii : By contacting Luscii or their healtcare provider. They are informed of the process via the privacy notice. Depending on the nature of the request and of what has been agreed on the DPA, Luscii will proceed direclty to the request or redirect the request to the healtcare provider
Will any information be sent outside **Luscii vitals** computer networks? If YES please give details of security controls in place
Explain how you will comply with the rights of data subjects
The Right to be Informed: a data subject has the right to be given information about how their data is being processed and why
How will you inform data subjects what you are doing with their data when you obtain it from them ? Centric Health will have a brief description on COVID 19 page and will update the privacy policy. In the update Centric Health will supply link to Luscii Vitals privacy policy.
How will you inform data subjects what you are doing with their data when you obtain it from someone else)?

Centric Health will provide notice on website, Privacy Statements for both Centric Health & Luscii . Details of this App will be discussed by Doctors and appointed administrative staff on the phone.

The Right to Access: a data controller must provide a data subject with confirmation as to whether or not personal data concerning him/her are being processed, and where this is the case, access to the data free of charge within one month of the request

How will you identify and retrieve all information in a system that relates to a data subject?

Centric Health will deal with SAR under current legalisation.

The Right to Rectification: a data controller is entitled to have their personal data rectified if inaccurate or incomplete

If a data subject asks for inaccurate data about them to be corrected, how would you achieve this?

Centric Health DPO will action.

Luscii : By contacting Luscii or their healtcare provider. They are informed of the process via the privacy notice. Depending on the nature of the request and of what has been agreed on the DPA, Luscii will proceed direclty to the request or redirect the request to the healtcare provider.

The Right to Erasure: applies where it is no longer necessary to process the personal data or the data subject withdraws their consent where no overriding lawful grounds apply

If a data subject asks for their data to be erased, how would you achieve this?

DPO will examine each case individually . Centric Health as a healthcare provider may need to defend themselves in a court of law , therefore will site Article 17 3 (e)

Luscii : By contacting Luscii or their healtcare provider. They are informed of the process via the privacy notice. Depending on the nature of the request and of what has been agreed on the DPA, Luscii will proceed direclty to the request or redirect the request to the healtcare provider.

If a data subject asks you to restrict further processing of their data (e.g. until a complaint or request to correct inaccurate data has been resolved, or to prevent scheduled deletion until they have obtained a copy of the data) how will you comply with this?

Patient should contact DPO@centrichealth.ie

The Right to Data Portability: applies only where processing is based on consent or contract and allows a data subject to obtain and reuse their personal data across different services for their own purposes

How can a data subject be provided with a machine readable copy of the personal data he or she has provided

Currently patients can not be provided with this . Centric Health will either print off notes , scan and securely e-mail (password protect) . Centric Health can provide this service to other GP who use Healthmail

Luscii : By contacting Luscii or their healtcare provider. They are informed of the process via the privacy notice. Depending on the nature of the request and of what has been agreed on the DPA, Luscii will proceed directly to the request or redirect the request to the healtcare provider.

Consent: applies only where processing is based on consent.

If a data subject withdraws their consent for their data to be processed for specific purposes, what would you have to do to comply with this?

support@luscii.com.

Automated Individual Decision-making, Including Profiling: a data subject has the right to obtain human intervention, express his or her point of view and to contest the decision.

Does the system make automated decisions about data subjects that may have a significant impact on them? Y N – if Y give details .

No

INTERNATIONAL TRANSFERS

Not applicable – all data is processed within the EEA and The GDPR applies

OTHER RISKS

What are the risks in relation to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the data in storage, in transit, and when in use?

Please see section under Security.

Resilience

How often will the system data be backed up?

Please see section under Security.

Where will the backup data be stored?
Please see section under Security.

How quickly can access be restored following disruption of service?

Please see section under Security.

Outline training and instructions necessary to ensure that users:
• Understand potential security risks;
• Understand their responsibilities and how to apply these;
• Understand what actions they need to take to protect the data.

Training will be provided by designated administration Doctor and Nurse trainers from Core Group.

Will the system have security logs?

Please see section under Security

Other notes to terms:

Luscii and Centric Health acknowledge that for the purposes of the Data Protection Act 1988, 2003, 2018 and GDPR, Luscii is the Data Processor and Centric Health is the Data Controller in respect of Patient(s) Data

Centric Health will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Patient's Personal Data via Luscii for the duration and purposes of the Service

Ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Patient(s) Data and against accidental loss or destruction of, or damage to, Patient(s) Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures;

Ensure that all Luscii staff who have access to and/or process Patient(s) Data are obliged to keep the Patient(s) Data confidential

Luscii will notify Centric Health without undue delay on becoming aware of a Personal Data Breach and no later than 24 hours. Centric Health will log any data breach through their DPO to the Irish Data Protection Commissioners Office within 72 hours of notifiable breach

Your Data Protection Rights;

Request information about whether we hold personal information about you, and, if so, what that information is and why we are holding/using it.

Request access to your personal information (commonly known as a "Data Subject Access Request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. Where you as a Patient require information about your health Centric Health you should address your Data Subject Request to your Centric Health practice.

Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing.

Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

Object to automated decision-making including profiling, that is not to be the subject of any automated decision-making by us using your personal information or profiling of you.

Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

Request transfer of your personal information in an electronic and structured form to you or to another party (commonly known as a right to “data portability”). This enables you to take your data from us in an electronically useable format and to be able to transfer your data to another party in an electronically useable format.

Withdraw consent: where we rely on consent as a legal basis, you may withdraw consent at any time by contacting us. Withdrawal of consent shall be without effect to the lawfulness of processing based on consent before its withdrawal.

In the event that you wish to make a complaint about how your Personal Data is being processed by Centric Health or how your complaint has been handled, you have the right to lodge a complaint directly with the supervisory authority who can be contacted as follows:

Contact: Data Protection Commissioner
Telephone: +353 57 8684800/+353 761 104 800
Post: Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, R32 AP23 Co. Laois
Or :
21 Fitzwilliam Square South, Dublin 2 . D02 RD28