LIVI DPIA – Our Health Partnership

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The project aims to provide GP practices with a video consultation solution. The proposed pilot solution will be provided by Livi, the parent company of which is Webbhälsa. Patients will sign up for the Livi app, entering personal details, then verify their identity via supply of photo ID documents and facial photo. Onfido process the identity verification documents on behalf of Livi. Patients may also upload a text description of presenting symptoms, and photographs relating to symptoms. The video consultation itself is not recorded or stored. GPs enter the consultation notes in the usual way, directly into the clinical system. The need for a DPIA was identified as there will be:- • Implementation of a new technology • Processing of special category data, including biometric data • Use of automated decision-making (biometric identifiers processed via AI) to make decisions on access to the service

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

All data, apart from that publicly available, will be collected from the user via user submission when they sign up to the app. Publicly available data will be collected manual from online sources, if required for fraud investigation.

Personal information is processed to set up a user account, authorize log in, maintain correct and up-to-date user information.

Personal identification information (ID docs, photograph, video) will be processed for the purposes of identity verification and fraud detection.

Information relating to medical symptoms and history, submitted by the user in the app, is processed for the provision of healthcare. This information may be shared with other healthcare providers directly related to provision of healthcare. For example, if a patient requires referral to a consultant following their Livi appointment, their information may be shared with the consultant.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data collected includes both personal and special category data (health and biometric).

Data collected will include:

- Personal details (name, ID number, address, email address, telephone number etc)
- Special category data (health, biometric details from photos and photo ID, video of user)
- Technical information (IP address, login information, type and version of operating system and unit, time settings, language settings, cookies, device identifiers)
- Information about user interaction with the service (keystrokes, times of when information is submitted)
- Publicly available user identity information

Personal details and identification data will be collected on first use of the app. Health data (ie. Symptoms) will be collected at each appointment.

Technical information may be collected regularly whenever the user interacts with the app.

Publicly available user identity information will be collected on sign up to the app for fraud investigation (if required) or for ongoing fraud investigations identified.

Livi retention period: information is kept for as long as necessary to be able to provide services to the user, or in order to fulfill legal obligation. User (personal) data is anonymised or erased in no later than 6 months from the time of which the user closes their account with Livi, unless necessary in order to enforce legal claims.

User data that has fulfilled the purpose for which it was collected and is no longer needed for the performance and development of the services or to ensure quality, is either anonymised or erased automatically.

User data provided with consent is removed at the time consent is withdrawn.

Onfido retention period: information is kept until request is made by the client (Livi), unless required for a legitimate such as a binding legal order not to destroy the information.

The number of individuals affected are those utilizing the Livi app.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Relationship:

Webbhälsa (parent company of Livi) is the controller for the processing of personal data (until a user commences contact with a healthcare provider). The Healthcare Provider is responsible for processing of personal data carried out in connection to patient use of the services.

Personal data is processed by Webbhälsa according to the instructions of the Healthcare Provider.

User Control:

Users can choose whether to sign up the app.

(Livi) Users maintain the rights to:

Request access to and information about the personal data which is being processed in conjunction with their use of the app/services

Ask for information about themselves to be corrected

Request that their personal data be erased (unless there is a legal obligation to retain patient data)

Ask to restrict processing of data: they believe to be inaccurate or the processing of which they believe to be unlawful

Object to processing of data where legal justification for the processing if legitimate interest

Withdraw consent where data has been given with consent

Data portability

(Onfido) Users can request:

Access a copy of their information

To have their information deleted

Exercise control over how their information is used

Vulnerable Group Access

Both children and vulnerable adults would have potential access to sign up to the app. Appointments can be booked on behalf of children aged 2-16 years.

Onfido's information security management system is ISO27001:2013 compliant.

Livi encrypts all data, and ensures user identity is verified by Onfido and GP identity is verified via their smartcard. Livi employ automatic and manual testing, auditing by independent third parties, and in house experts to maintain security.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Purposes of processing:

Webbhälsa (parent company of Livi) is the controller for the processing of personal data (until a user commences contact with a healthcare provider), necessary for the performance of their contract, for the purposes of:

a) to process user application or terminate user account in the App

b) to provide you with authorization to login and use your user account

c) verify age and identity

d) to maintain correct and up-to-date user information

e) for user to be able to monitor and administer ongoing care matters

f) to handle user choice of settings and information about payment

g) to otherwise be able to provide the Services to you according to our General Terms and Conditions

Onfido, who are contracted to undertake identity verification services on behalf of Livi, process information for the purposes of:

a) identity verification

b) fraud detection

c) analysing how users interact with the service

d) to develop Identity Verification Services

Effect on individuals: Patients easily able to access video consultations via a secure platform, allowing appointment availability during the extended access hours without travel.

Benefits: ability for GPs to conduct remote consultations without the patient present allows GP to work from home. Patients unable to physically access the surgery for an appointment due to physical or time constraints are able to access appointments.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Consultation will be sought with: the OHP governance committee to identify the risks associated with the pilot. the OHP board members to share the DPIA for the pilot. the technical teams of Livi and Onfido to clarify any points concerning the DPIA, such as third party affiliates information is shared with. OHP legal advisors

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Lawful basis: Livi/Webbhälsa process data, as it is necessary for them to fulfill their contractual obligations (GDPR Article 6). User Data (non-medical information) is also processed, under the basis of legitimate interest of improving user experience in the app, for direct marketing including user analysis, such as age, place of residence, and how the patient uses the service. Onfido process data on the basis that the user has requested Identity Verification Services, the client has a legitimate or lawful reason for requesting Identity Verification Services, it is in the legitimate interest of the client and Onfido for Onfido to use the information to develop Identity Verification Services, the processing is necessary to carry out a task in the public interest, or for reasons of substantial public interest, the processing is for scientific research purposes, or the user has provided their consent.

The Healthcare Provider processes special category data for the purpose of providing healthcare (GDPR Article 9 - purpose of preventive or occupational medicine).

Step 5: Risk mitigation

Ref. no	Description of the risk	Rationale and consequences	Existing controls that contribute to and manage risks identified	Assessment of residual current risk	Recommended mitigations or privacy enhancements	Residual risk remaining despite new safeguards
001	Unauthorized information access by leading to identity fraud/theft of user, reputational damage of user, blackmail of user	Livi admin team and GPs have access to patient record and details entered during app sign up.	Access restricted to those providing patient with healthcare, or as part of Livi's ongoing quality assurance and product development. Information is safeguarded at Livi. Utilisation of in-house experts, automatic and manual testing and regular audits by independent third parties of security measures. Auditable role based access. GP login with smartcard. All info at Livi heavily encrypted. Onfido ISMS ISO27001:2013, data encryption using AES-256	Low	None	Low
002	Login by party other than user to app	Stolen phone, attempted sign up as another person, attempted login by others with access to the mobile	Identity verification using biometric data at point of sign up. Login security measures and ability to sign out	Low	Patient to not use auto-login and follow sign out instructions	Low
003	Patient unable to access app	Livi requires iOS v10.0 or later and Android v6.0 or later	Livi support phoneline available	Medium	Inform patients of technical requirement	Low
004	Patient identity unable to be identified	No photo ID available/automatic processing used for identity verification	Normal appointments still available to patients if unable to access digital consultations. Make patients aware of sign up process for Livi	Low	N/A	Low

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Naomi Frazer, DPO, 1/5/2019	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Leanne Hoye, DPO, 1/5/2019	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	N/A, approved by DPOs	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: None		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons

Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Naomi Frazer	The DPO should also review ongoing compliance with DPIA