BEACON MEDICAL SYSTEMS LIMITED
Company number **14638585**
5 New Street Square, London, United Kingdom, EC4A 3TW

Health and care:
Data Protection Impact Assessment (DPIA)

January 2023	5.0	Claire Robinson	Create formalised Data Protection Impact Assessment.
June 2024	6.0	Claire Robinson	Review Data Protection Impact Assessment to follow NHS guidance.
November 2024	6.1	Claire Robinson	Update 13th November 2024 to align with updated IG FAQ guide, clarify role of processor / controller, add in further hyperlinks for clarity, updated formatting and incorporate data points captured by the addition of the profiles feature (for which there is a separate DPIA).
January 2025	6.2	Claire Robinson	Correct typo, add clarification around the use of biometrics for logon purpose.

Introduction

This document details the data protection impact assessment (DPIA) carried out by Beacon Medical Systems Ltd with regard to the use of Pando as a mobile and/or web application at any given NHS trust, hospital, community care setting, GP surgery or other organisation.

Purpose:

The purpose of a data protection impact assessment is to identify any new collection or uses of potentially sensitive data, to assess the possible risks associated with these and to allow organisations to make an informed decision about the technologies they employ with regards to data collection, use, or sharing.

Scope

This data protection impact assessment relates to the use of Pando as a mobile and/ or web application within a clinical /healthcare/community setting. It refers to the current data protection laws as they stand, although it will continue to be reviewed regularly to take into consideration ongoing regulatory change. Beacon Medical Systems Ltd reserves the right to update this data protection impact assessment as necessary, particularly with regard to the changing landscape of data protection law.

Background

A data protection impact assessment (DPIA) will help you to identify and mitigate potential data protection risks to an acceptable level before using or sharing (processing) data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

- Data protection by design - privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.
- Accountability - your organisation is responsible for showing how it complies with data protection laws.
- Transparency - personal data must be used and shared in a transparent way.
- Security - adequate measures need to be in place to protect data. This can range from policies and procedures to technical security measures such as encryption of data.

DPIAs are mandatory when there is a high risk to individuals, such as when using the health and care data of a large number of people. However, health and care organisations are strongly advised to complete a DPIA when using and sharing personal data in a new or substantially changed way.

A DPIA involves a risk assessment. If a high-level risk remains after applying mitigations, then you must consult with the Information Commissioner's Office (ICO) for further advice before starting to collect, use or share the data.

This DPIA is a live document – we will update it if there are any changes to:

- the purpose - why we are proposing to use or share personal data
- the manner - how we will use or share the data
- who is involved - the organisations using and sharing personal data

Contents

1 Screening questions

1.1 Do you need to do a DPIA?

In summary, Pando is a smartphone application and communication tool for clinical teams. Below are the key features/uses of Pando.

- Secure, compliant instant messaging, including sharing of photos and files
- Live task management and workflow tracking
- Sharable patient profiles & patient lists
- Hospital directory function with profiles of users (see separate DPIA).
- Forums feature.
- Video consultations for some clients (see separate DPIA).

We have considered whether we need a DPIA and as the personal data used on the application securely transfers and stores private health records and is likely to raise privacy concerns, we have identified a need to create and update a DPIA for the Pando application.

1.2 Summary of how data will be used and shared

Pando do not have a direct relationship with the data subject and the data subjects have as much control over their data when their clinician uses Pando as they do in any other situation where their Article 9 data is handled by their healthcare provider. The stipulated and expected use is instant messaging not as the core patient record.

Pando operates a Client-Server model – sharing data, including personal patient data, over SSL encrypted links (256-bit) using Internet connections provided by Trust (or other appropriate Wi-Fi when clinicians are roaming on-site) or 3G/4G/5G. Data is securely transmitted, processed and stored on the Pando infrastructure. Retention is governed by the appropriate retention schedules.

1.3 Description of the data

☒	Personal data [individuals can be identified]
□	Pseudonymised data [identifiers, for example name or NHS number, are replaced with a unique number or code (a pseudonym)]
☒	Anonymous data [not identifiable, for example trends or statistics]

2 Why do you need the data?

2.1 What are the purposes and benefits for using or sharing the data?

Pando is a smartphone application and communication tool for clinical teams. Pando has been purpose-built for medical staff and is designed to support high-quality, secure and compliant instant messaging for individuals or groups. Available for both iOS and Android, the app has a few simple key features:

- Secure, compliant instant messaging, including sharing of photos and files
- Live task management and workflow tracking
- Sharable patient profiles & patient lists
- Hospital directory function
- Forums feature.
- Video consultations for some clients (see separate DPIA).

Modern clinical and community care is fast-paced, and increasingly complex as clinical teams deal with a higher volume and turnover of patients whose care typically involves multiple tests and interventions. As a result, teams must collaborate ever more closely to deliver high quality care. This is currently difficult to achieve since hospital communication systems rely on technology from the 1970s such as pagers, telephone switchboard and printed lists of patients; our belief as clinicians ourselves, and from survey data collected from over 120 doctors, is that these tools are not fit for purpose in the modern NHS. Busy NHS clinicians (and their associated supporting colleagues) are rarely desk-bound with immediate access to a desktop PC or laptop whilst delivering, managing, or planning patient care.

Messaging systems such as WhatsApp are suboptimal because of the IG and data protection challenges that they pose. It is difficult to ensure that their use complies NHS DSP Toolkit Guidelines, and the Data Protection Act 2018. Meta who owns WhatsApp have been subject to many privacy issues and fined by the regulatory authorities for violations.

Pando additionally provides high-levels of technical data security assurance such as high levels of encryption in transit and at rest (minimum AES 256-bit standard for data encryption in-transit and at-rest). In transit data is encrypted and transferred via HTTPS (TLS v 1.2 min) protocol. When transmitting messages devices use an SSL handshake with 2048-bit RSA keys to encrypt the socket connection to Pando servers. The infrastructure supports the sync of RSA public keys. To further enhance security OWASP certificate pinning has been implemented and access to Pando servers is only possible via SSH keys.

3 What data do you want to use or share?

○

3.1 Can you use anonymous data for your purposes? If not, explain why.

☐	Yes
☒	No
☐	Unsure

No, anonymous data wouldn't be suitable for the purposes of Pando. Pando is designed to assist healthcare professionals in their clinical workplace, which involves handling sensitive healthcare data. While anonymous data might be useful in some contexts, it wouldn't serve our intended purpose, which is to facilitate communication and collaboration among healthcare professionals regarding patient care.

The data handled by Pando is directly related to patient care and contains sensitive information about individuals' health conditions and treatments. This data is necessary for healthcare professionals to provide effective care to their patients.

Pando remains the data processor for the patient’s personal or identifiable data, and it is encrypted when stored by us.

3.2 Which types of personal data do you need to use and why?

Patient data (input by healthcare professionals): Please note that Pando is the processor for this data.

☒	Forename	☒	Physical description, for example height	☒	Photograph / picture / of people
☒	Surname	☒	Phone number	☐ ☒ ☐	Location data e.g. IP address (aggregated) Other
☒	Address	☒	Email address	☐	Audio recordings
☒	Postcode full	☒	GP details	☒	Video recordings
☒	Postcode partial	☒	Legal representative name (personal representative)	☒	Other Free form notes that may include other personal data.
☒	Date of birth	☒	NHS number	☐	None
☒	Age	☒	National insurance number		
☒	Gender	☒	Another numerical identifier		

In addition to the data that we currently capture when data is input by users into the app, we capture the following data about our users themselves. Pando is the data controller for this data flow. There is a separate DPIA available which documents this data flow for profiles of users.

Facility/Affiliation: this represents the clinic/hospital/surgery a user works at e.g. ‘Frimley Park Hospital’. Data will be stored as a table of facility names.

Bio and Notes: these are non-mandatory free text fields. The use for these fields is at the discretion of the user.

Special Interests: to replace the current free-text Specialty field. Users can select multiple, granular options relating to their clinical areas of interest or expertise.

Profile Picture: a non-mandatory image.

GMC Number: captured only for users that state their role as Doctor.

Speciality/Care Setting: Dominant Clinical Specialty, or Care Setting depending on which is applicable to the user. An example may be 'Psychiatry: Medical Psychotherapy'

There have been no changes to the following data fields already stored within the app against a user's profile:

- Organisation
- Name
- Role
- Email
- Phone
- Ask Advice Teams

An overview of all data points captured about users of the Pando App:

Data	**Mandatory ?**	**Displayed on user's profile?**	**Captured during onboarding?**
Facility/Affiliation	no	yes	yes
Bio	no	yes	no
Notes	no	yes	no
Special Interests	no	yes	yes
Profile Picture	no	yes	no
GMC Number	no	yes	where applicable
Specialty/Care Setting	yes	yes	yes
Organisation	yes	yes	yes
Role	yes	yes	yes
First Name	yes	yes	yes
Surname	yes	yes	yes
Email	yes	at discretion of user	yes
Phone	yes	at discretion of user	.

Ask Advice Teams	n/a	yes	no

3.3 Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?

Type of data		Reason why this is needed (leave blank if not applicable)
☒	Information relating to an individual's physical or mental health or condition, for example information from health and care records	Pando is designed to be used by trained healthcare professionals in their clinical workplace. Patients would expect their data to be processed as part of their ongoing care and Pando is a tool that assists healthcare professionals.
☒	Biometric information in order to uniquely identify an individual, for example facial recognition	ONLY for app login where a user chooses to enable this on their device.
☒	Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	This data is not needed however may be processed when necessary to provide individual care.
☒	Information relating to an individual's sexual life or sexual orientation	This data is not needed however may be processed when necessary to provide individual care.
☒	Racial or ethnic origin	This data is not needed however may be processed when necessary to provide individual care.
☐	Political opinions	
☐	Religious or philosophical beliefs	
☐	Trade union membership	
☐	Information relating to criminal or suspected criminal offences	

3.4 Who are the individuals that can be identified from the data?

☒	Patients or service users
☒	Carers
☒	Staff

☐	Wider workforce
☐	Visitors
☐	Members of the public
☐	Other

○

○

3.5 Where will your data come from?

The data for Pando primarily comes from healthcare professionals using the platform in clinical settings. The data includes personal patient data, which is transmitted, processed, and stored on the Pando infrastructure.

The data originates from interactions between healthcare professionals, such as messages, notes, and discussions related to patient care. This can include sensitive information about patients' health conditions, treatments, medications, test results, and other relevant clinical data.

3.6 Will you be linking any data together?

☒	Yes
☐	No
☐	Unsure

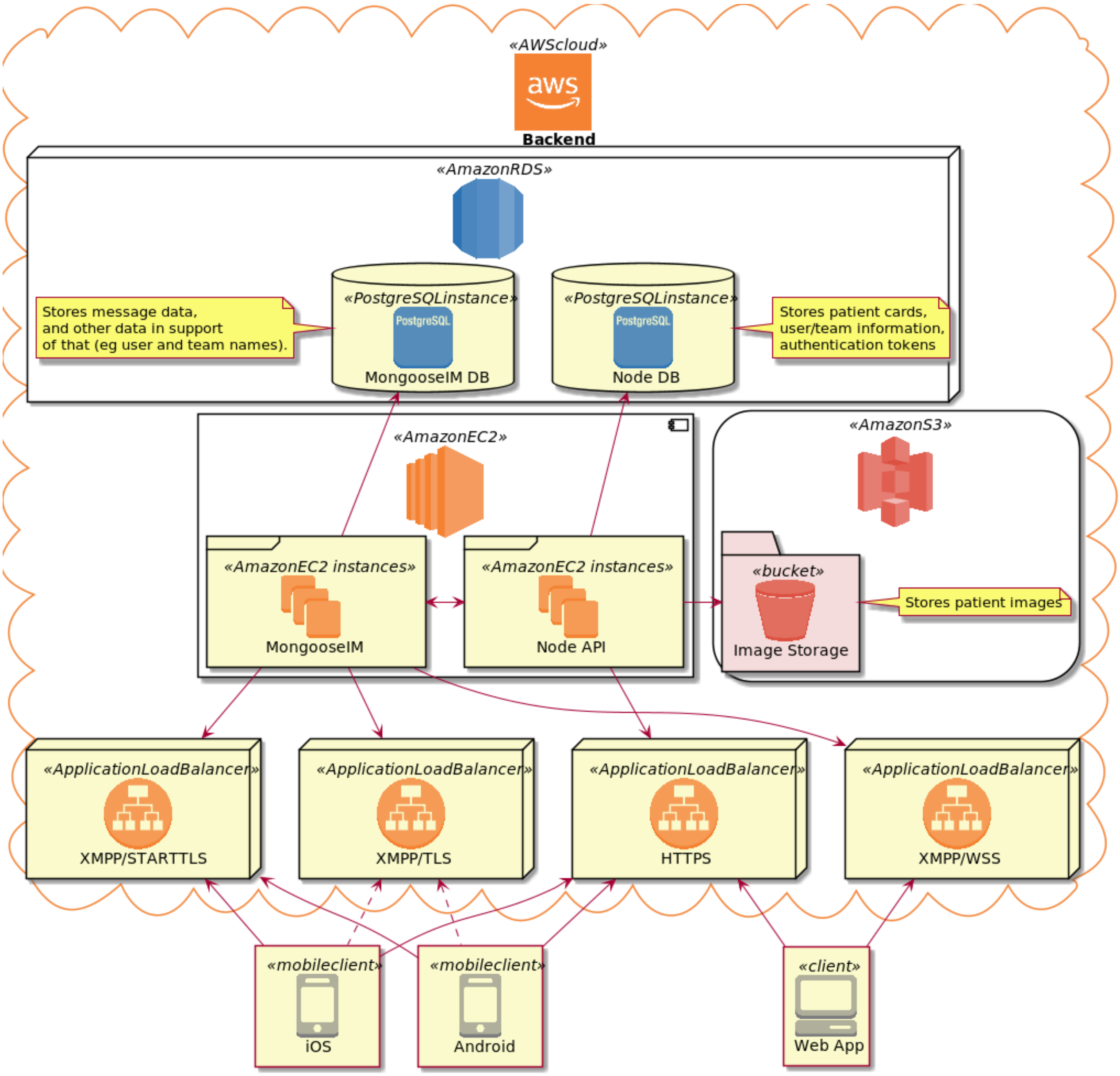
○

3.7 Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?

☐	Yes
☒	No
☐	Unsure

Data is linked in order to validate an NHS user using their email address.

4 Where will data flow?



Tabular Data Flows and Security

Flow Ref	***Flow Name***	***From***	***To***	***Method***	***Security Controls***	***Storage***
1	***Image Access***	***Node API***	***Apps***	***System Access (HTTPS)***	***TLS / ABAC***	***On-device cache***
2	***Image Send***	***Apps***	***Node API***	***System Transfer (HTTPS)***	***TLS / ABAC***	***AWS S3 Encrypted Storage***
3	***Message Transmit***	***Apps***	***MongooseIM***	***System Transfer (XMPP)***	***TLS / ABAC***	***AWS RDS Encrypted Database***
4	***Message Receive***	***MongooseIM***	***Apps***	***System Transfer (XMPP)***	***TLS / ABAC***	***On-device cache***
5	***Metadata Access***	***Node API***	***Apps***	***System Access***	***TLS / ABAC***	***On-device cache***
6	***Metadata Store***	***Apps***	***Node API***	***System Transfer***	***TLS / ABAC***	***AWS RDS Encrypted Database***
7	***Patient Data Access***	***Node API***	***Apps***	***System Access***	***TLS / ABAC***	***On-device cache***
8	***Patient Data Store***	***Apps***	***Node API***	***System Transfer***	***TLS / ABAC***	***AWS RDS Encrypted Database***

General Notes:

- Pando uses TLS to provide Confidentiality, Integrity, and System-level Authentication for all connections both internally and externally.
- User-level Authentication operates by limited-lifetime access tokens which are proven via OAuth or by an authentication token code sent via email.
- Pando uses fine-grained access controls based on Identity, Network and Team membership, Patient assignment, and previous sharing actions such as Image messages, forming an Attribute-Based Access Control system with a bespoke policy driven by code.
- The on-device cache may be encrypted or in-memory only, depending on platform.

1. Image Access - The mobile and web applications access images in messages by reference, requesting them from our API. Such access is communicated over TLS, and access-controls are in place within the API. Images are stored encrypted on the AWS S3 system, and after access may be held in on-device cache.
2. Image Send - Pando Apps upload images either directly from the camera subsystem or via the Image Gallery. The sender sets access-control requirements in terms of Team or Identity. Images uploaded to Patient cards have access controls implicitly based on access to the Patient. Images held within the Image Gallery are held on the device within the application filesystem area.
3. Message Transmit - Pando Apps send messages via XMPP. Message destinations are checked under RBAC rules. Messages are archived under long-term retention policy on an AWS RDS encrypted database and may be held in on-device cache.
4. Message Receive - Pando Apps receive messages via XMPP. Message destinations are checked under RBAC rules. Messages are archived under long-term retention policy on an AWS RDS encrypted database and may be held in on-device cache.
5. Metadata Access - Metadata about images, group membership, etc is accessed via the Node API by Pando Apps. The metadata includes the information used for access control decisions. The information may be held in on-device cache.
6. Metadata Store - When storing changes to metadata, Apps send this information to the Node API where (subject to access controls) it is stored in an AWS RDS encrypted database.
7. Patient Data Access - Data about Patients, etc is accessed in the same way as the metadata. The information may be held in on-device cache.
8. Patient Data Store - When storing patient data, Apps send this information to the Node API where (subject to access controls) it is stored in an AWS RDS encrypted database.

4.1 Confirm that your organisation’s information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.

☒	Yes
☐	No
☐	Unsure

4.2 Will any data be shared outside of the UK?

☐	Yes
☒	No
☐	Unsure

5 Is the intended use of the data lawful?

5.1 Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?

☐	(a) We have consent
☐	(b) We have a contractual obligation
☐	(c) We have a legal obligation
☒	(e) We need it to perform a public task *6(1)(e) "…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…".* *9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…"*
☐	(f) We have a legitimate interest

5.2 If you have indicated in question 3.3 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?

○

☐	(b) We need it to comply with our legal obligations for employment
☐	(f) We need it for legal claims, to seek legal advice or judicial acts
☐	(g) We need to comply with our legal obligations to provide information where there is a substantial public interest, as set out in this list
☒	(h) We need it to comply with our legal obligations to provide or manage health or social care services
☐	(i) We need it to comply with our legal obligations for public health
☐	(j) We need it for archiving, research and statistics where this is in the public interest

5.3 What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?

☒	Implied consent
☐	Explicit consent
☐	Section 251 support
☐	Legal requirement
☐	Overriding public interest

5.3.1 Please provide further information or evidence.

Not applicable

6 How are you keeping the data secure?

6.1 Are you collecting information?

☒	Yes
☐	No

6.2 How is the data being collected?

The data for Pando comes from healthcare professionals using the platform in clinical settings. Users input details about themselves, e.g. speciality, GMC number in order to ensure that their own data is accurate and up-to-date and to help other users to contact the correct individual.

Pando operates a Client-Server model – sharing data, including personal patient data, over SSL encrypted links (256-bit) using Internet connections provided by Trust (or other appropriate Wi-Fi when clinicians are roaming on-site) or 3G/4G/5G.

6.3 Are you storing information?

☒	Yes
☐	No

6.3.1 How will information be stored?

Storage location	
☐	Physical storage, for example filing cabinets, archive rooms etc
☐	Local organisation servers
☒	Cloud storage

6.4 Are you transferring information?

☒	Yes
☐	No

6.5 How will information be transferred?

In transit data is encrypted and transferred via HTTPS (TLS 1.2 min) protocol. When transmitting messages devices use an SSL handshake with 2048-bit RSA keys to encrypt the socket connection to servers. Also supports the sync of RSA public keys, ensuring high levels of encryption. To further enhance security - OWASP certificate pinning implemented and access to Pando servers is only possible via SSH keys.

6.6 How will you ensure that information is safe and secure?

Security measure		**Details (leave blank if not applicable)**
☒	Encryption	The data is encrypted in transit and at rest (following best practice as defined in ISO27001 ISMS).
☒	Password protection	Password protection (including BCrypt hashing) and multi factor authentication.
☒	Role based access controls (RBAC)	Access to patient identifiable data will be strictly limited.
☒	Restricted physical access	Access to data centres is strictly limited.
☒	Business continuity plans	Business Continuity and Disaster Recovery policies, procedures and testing as part of ISO 27001 preparation and alignment. .
☒	Security policies	Detailed in ISO27001 aligned ISMS.
☒	Other	DSP Toolkit to Standards Exceeded, Cyber Essentials Plus.

6.7 How will you ensure the information will not be used for any other purposes beyond those set out in question 2.1?

Specify the measures below which will be used to limit the purposes the data is used for.

[Put an ☒ next to all that apply and provide details.]

Security measure		Details (leave blank if not applicable)
☒	Contract	For example, a call off contract from GCloud etc.
☒	Data processing agreement	This sets out the arrangements between a controller and processor and is legally binding.
☒	Data sharing agreement	This sets out the arrangements for sharing data between the organisations involved – it may or may not be legally binding depending on the context.
☒	Data sharing and processing agreement (DSPA)	Where appropriately completed, this is a legally binding agreement that sets out the arrangements for processing and/or sharing data, and/or joint controller arrangements.
☒	Staff training	Users complete mandatory DSP training.
☐	Other	[please state]

7 How long are you keeping the data and what will happen to it after that time?

7.1 How long are you planning to use the data for?

All data will be stored in accordance with the Records Management Code of Practice for Health and Social Care 2021. However, we would delete the data earlier than suggested by this code if they were informed that the condition of Schedule 9(3) GDPR and s. 11(1) Data Protection Act 2018 no longer applies.

7.2 How long do you intend to keep the data?

Adult health records need to be kept for a minimum of 8 years from the time they were last used. The Records Management Code of Practice sets out the retention period for health and care records.

7.3 What will happen to the data at the end of this period?

Action		Details (leave blank if not applicable)
☐	Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction)	
☐	Permanent preservation by transferring the data to a Place of Deposit run by the National Archives	
☐	Transfer to another organisation	
☐	Extension to retention period	
☐	It will be anonymised and kept	
☐	The controller(s) will manage as it is held by them	
☒	Other	Review in conjunction with the data controller.

8 How are people’s rights and choices being met?

8.1 How will you comply with the following individual rights (where they apply)?

Individual right	How you will comply (or state *not applicable* if the right does not apply)

The right to be informed The right to be informed about the collection and use of personal data.		We have assessed how we should inform individuals about the use of data in relation to the Pando application. We consider the communications methods below meet this obligation.
	☒	Privacy notice(s) for all relevant organisations
	□	Information leaflets
	□	Posters
	□	Letters
	□	Emails
	□	Texts
	□	Social media campaign
	☒	DPIA published
	□	Other
	□	Not applicable
The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.	Pando will assist the controller in the event of a data subject requiring access.	
The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.	Pando will assist the controller in the event of a data subject requiring rectification.	
The right to erasure The right to have personal data erased, if applicable.	Not applicable in direct care. Pando will assist the controller if data is entered into the app in error and needs to be deleted.	

The right to restrict processing The right to limit how their data is used, if applicable.	Pando will act on the instructions of the controller.
The right to data portability The right to obtain and re-use their personal data, if applicable.	Not applicable.
The right to object The right to object to the use and sharing of personal data, if applicable.	Unlikely to be applicable in individual care. Pando will take instruction from the data controller.

8.2 Will the national data opt-out need to be applied?

☐	Yes
☒	No

8.3 Will any decisions be made in a purely automated way without any human involvement (automated decision making)?

☐	Yes
☒	No
☐	Unsure

8.4 Detail any stakeholder consultation that has taken place (if applicable).

Various consultations with health care professionals over the last decade.

9 Which organisations are involved?

9.1 List the organisation(s) that will decide why and how the data is being used and shared (controllers).

It is important to note that Pando is not the data controller – the data controller is the employer of the user (e.g. clinic, GP surgery, hospital, care home etc.). Our users (clinicians, healthcare, care workers using the service with patients)

NHS England has advised healthcare organisations to process patient data for the delivery or administration of care under the following legal bases:

6(1)(e) "…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…".

9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…"

For the purposes of processing patient data Pando is acting under the instructions of the user's organisation and it is the organisation (data controller) that determines the lawful basis for processing. in most cases the organisation is using Article 6 (1) (e) (processing in the exercise of official authority vested in the controller). available here.

9.2 List the organisation(s) that are being instructed to use or share the data (processors).

Pando acts under instruction from those listed in question 9.1, for example they are likely to be told:

- what data to collect
- who to collect data from
- how the collection is legal
- the purpose for the collection
- who to share the data with
- how long to keep the data

9.3 List any organisations that have been subcontracted by your processor to handle data

Pando is hosted on London Cluster's secure ISO27001 certified AWS servers. Other organisations that act as sub processors for the support and development of the Pando product are listed on our website.

9.4 Explain the relationship between the organisations set out in questions 28, 29 and 30 and what activities they do

AWS host the data. For other details please see 9.3 and 3.6.

9.5 What due diligence measures and checks have been carried out on any processors used?

Due diligence measures		Details (leave blank if not applicable)
☒	Data Security and Protection Toolkit (DSPT) compliance	To standards exceeded.
☒	Registered with the Information Commissioner's Office (ICO)	
☒	Digital Technology Assessment Criteria (DTAC) assessment	

10 What data protections are there and what mitigations will you put in place?

10.1 Complete the risk assessment table. Use the risk scoring table to decide on the risk score.

Risk assessment table

Risk ref no.	**Description**	**Risk score* (L x I)**	**Mitigations**	**Risk score* with mitigations applied**
01	**Staff mobile devices lost or stolen –** subset of PID digital records no longer secured	16	(1) No PID stored permanently on individuals' devices- images, tasks, patient profiles are at all times pulled down from our servers. Encrypted at rest and in transit. (2) PIN code lock-down of all mobile devices at 15 minutes maximum. Time out cannot be changed by user. (3) Remote Wipe function is included in common Exchange/ActiveSync environments, free on iOS/Android and EMM (Enterprise Mobile Management) systems are also available.	4
02	**PID digital records intercepted over internet connections**	9	(1) Server-Side Encryption (SSE), using 256-bit Advanced Encryption Standard (256-bit AES) in transit and at rest. (2) In transit data is encrypted and transferred via HTTPS (TLS 1.2 min) protocol. When transmitting messages devices use an SSL handshake with 2048-bit RSA keys to encrypt the socket connection to servers. Also supports the sync of RSA public keys. To further enhance security - OWASP certificate pinning implemented and access to Pando servers is only possible via SSH keys. (3) Strong Password policy enforced.	4
03	**PID digital records stolen from server platform**	6	(1) Insider-hacking threat eliminated; no readable PID by any system admin or developer ('data privacy by default' methodology) if an unauthorised database extraction occurs. (2) Internet-based hacking threat significantly reduced by SPI and application-based firewall (layer-7), automated account lockouts (security policy) after three failed attempts, strong	2

			password enforcement (security policy) and AES-256 server data encryption. (3) Regular penetration testing carried out for both servers and smartphone application.	

***Risk scoring table**

		Impact (I)				
		Negligible (1)	**Low (2)**	**Moderate (3)**	**Significant (4)**	**Catastrophic (5)**
Likelihood (L)	**Rare (1)**	**1**	**2**	**3**	**4**	**5**
	Unlikely (2)	**2**	**4**	**6**	**8**	**10**
	Possible (3)	**3**	**6**	**9**	**12**	**15**
	Likely (4)	**4**	**8**	**12**	**16**	**20**
	Almost certain (5)	**5**	**10**	**15**	**20**	**25**

11 Review and sign-off

Reviewer sign-off	
Reviewer name:	Rob Cherry
Reviewer job title:	SIRO
Reviewer contact details:	rob.cherry@hellopando.com
Date of review:	November 2024
Comments:	Update 13th November 2024 to align with updated IG FAQ guide, clarify role of processor / controller, add in further hyperlinks for clarity, updated formatting and incorporate data points captured by the addition of the profiles feature (for which there is a separate DPIA).
Date for next review:	June 2025 or when a significant change is made to the Pando App.

Reviewer sign-off	
Reviewer name:	Claire Robinson
Reviewer job title:	Data Protection Officer
Reviewer contact details:	dpo@helloPando.com
Date of review:	January 2025

Comments:	Update 26th April 2024 to follow NHS guidance. Update 8th June to alter DPIA into new NHS IG template.
Date for next review:	June 2025 in advance of DSP submission or when a significant change is made to the Pando App.