Pando

Data Protection Impact Assessment

Introduction: This document details the data protection impact assessment (DPIA) carried out by Forward Clinical 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. Forward Clinical 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: It is necessary to complete at DPIA whenever a significant change is made to the way in which data is collected or processed by an organisation, to ensure that the impact of this on the data subject and their rights has been fully considered.

As described by the ICO, the steps involved in completed a data protection impact assessment are:

1. Identify the need for a DPIA.
2. Describe the processing/information flow.
3. Consultation process.
4. Assess necessity and proportionality.
5. Identify and assess risks.
6. Identify measures to reduce risks.

Table of Contents

Data Protection Impact Assessment (DPIA) 3

Data protection impact assessment screening questions 3

Step 1: Identify the need for a DPIA 3

Step 2: Describe the nature of the processing 5

Step 3: Consultation process 9

Step 4: Assess necessity and proportionality 9

Step 5: Identify and assess risks 10

Sign off and record the DPIA outcomes 12

Ongoing Review: Integrate the DPIA outcomes back into the project plan 13

Contact point for future privacy concerns 17

Data Protection Impact Assessment (DPIA)

Data protection impact assessment screening questions

These questions are intended to help decide whether this DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise.

Question	Answer *Please add any relevant comments*
Will the project involve the collection of new information about individuals?	No
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	No
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	Yes – encrypted transfer and secure storage (encryption of data when at rest and access authentication) of private health records. There is a universal privacy expectation that highest levels of information security will be deployed.
Will the project require you to contact individuals in ways that they may find intrusive?	No

Step 1: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

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.

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.

Public email platforms such as Google Mail, Office 365 etc. have either been deemed unsuitable due to limited functionality or non-compliance with NHS Digital data security policies, NHS DSP Toolkit Guidelines, and the Data Protection Act 2018.

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.

Step 2: 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?

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?

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. Please refer to Pando Data flows.

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)?

Pando is designed to be used by trained healthcare professionals in their clinical workplace (e.g. clinic, hospital, care home, hospice, GP surgery etc.).

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.

Patients would expect their data to be processed as part of their ongoing care and Pando is a tool that assists healthcare professionals.

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)

The Information Governance Alliance, NHS X and NHS Digital 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.

Pando is owned by Forward Clinical Ltd who are registered with the ICO and have appointed a Data Protection Officer (DPO).

Pando is hosted on London Cluster's secure ISO27001 certified AWS servers.

Pando submitted DSP Toolkit in June 2021 obtaining standards exceeded and has Certification including Cyber Essentials Plus.

Device and Usage Data – Revision to Privacy Policy - April 2020 (requested by NHS X).

We use common information-gathering tools, such as tools for collecting usage data, cookies, web beacons and similar technologies to automatically collect information that may contain Personal Data from your computer or mobile device as you navigate our websites, our services or interact with emails we have sent to you.

As is true of most websites, we gather certain information automatically on connection with the use of the website by individual users. This information may include IP address (or proxy server), device and application identification numbers, location, browser type, Internet service provider and/or mobile carrier, the pages and files viewed, searches, operating system and system configuration information and date/time stamps associated with your usage. This information is used to analyse overall trends, to help us provide and improve our websites and Apps and to guarantee their security and continued proper functioning.

In addition, we gather certain information automatically as part of your use of the cloud products and services. This information may include IP address (or proxy server), device and application identification numbers, location, browser type, Internet service provider and/or mobile carrier, the pages and files viewed, searches and other actions you take, operating system and system configuration information and date/time stamps associated with your usage. This information is used to maintain the security of the services, to provide necessary functionality, as well as to improve performance of the services, to assess and improve customer and user experience of the services, to review compliance with applicable usage terms, to identify future opportunities for development of the services, to assess capacity requirements, to identify customer opportunities and for the security of Pando generally (in addition to the security of our products and services). Some of the device and usage data collected within the services, whether alone or in conjunction with other data, could be personally identifying to you. Please note that this device and usage data is primarily used for the purposes of identifying the uniqueness of each user logging on (as opposed to specific individuals), apart from where it is strictly required to identify an individual for security purposes or as required as part of our provision of the services to our customers (where we act as a Processor).

We use cookies and similar technologies such as web beacons, tags and JavaScript, alone or in conjunction with cookies, to compile information about the usage of our websites and interaction with emails from us.

When you visit our websites, we or an authorised third party may place a cookie on your browser and/or device, which collects information, including Personal Data, about your online activities over time and across different sites. Cookies allow us to track usage, determine your browsing preferences and improve and customise your browsing experience.

We use both session-based and persistent cookies on our websites. Session-based cookies exist only during one session and disappear from your computer when you close your browser or turn off your computer. Persistent cookies remain on your computer or device after you close your browser or turn off your computer. To change your cookie settings and preferences for the site you are visiting, click the Cookie Preferences link. You can also control the use of cookies at the individual browser level but choosing to disable cookies may limit your use of certain features or functions on our websites and services.

The following describes how we use different categories of cookies and similar technologies and your options for managing the data collection settings of these technologies:

Type of Cookies	Description	Managing Settings
Required cookies	Required cookies are necessary for basic website functionality. Some examples include session cookies needed to transmit the website, authentication cookies, and security cookies. If you have chosen to identify yourself to us, we may place on your browser a cookie that allows us to uniquely identify you when you are logged into the websites and to process your online transactions and requests.	Because required cookies are essential to operate the websites and the Pando desktop web App, there is no option to opt out of these cookies.
Functional cookies	Functional cookies enhance functions, performance, and services on the website. Some examples include: cookies used to analyse site traffic, cookies used for market research, and cookies used to display advertising that is not directed to a particular individual. Functional cookies may also be used to improve how our websites function and to help us provide you with more relevant communications, including marketing communications. These cookies collect information about how our websites are used, including which pages are viewed most often. We may use our own technology or third-party technology to track and analyse usage information to provide enhanced interactions and more relevant communications, and to track the performance of our advertisements. For example, we use Google Analytics ("Google Analytics"), a web analytics service provided by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. You can learn about Google's privacy practices by going to www.google.com/policies/privacy/partners/ . Google Analytics uses cookies to help us analyse how our websites are used, including the number of visitors, the websites from which visitors have navigated to our websites, and the pages on our websites to which visitors navigate. This information is used by us to improve our websites. Pando may also utilise HTML5 local storage or Flash cookies for the above-mentioned purposes. These technologies differ from browser cookies in the amount and type of data they store, and how they store it.	You can choose to opt out of functional cookies. To change your cookie settings and preferences, click the Cookie Preferences link

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?

- Engagement with relevant IG managers/CIO/CCIO at Trust with relevant team members from Forward Clinical Ltd.
- Engagement with Forward Clinical Ltd (app developer and service provider)
- Consultation is performed via internal team meetings, discussions with our initial NHS consultant users, reviewing the service provider's ISMS (Information Security Management System), Information Security Policy, Privacy Policy and SLAs (Service Level Agreements)/EULAs (End User License Agreements) and discussing technical requirements with the service providers to seek relevant assurances.
- Maintenance of information assets register and information security risk assessment and clinical hazards log.

Step 4: Assess necessity and proportionality

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?

- Forward Clinical Ltd are not the data controllers of the patient data; they are the processors.
- Other methods of communicating / processing are likely to be fundamentally secure than using the Pando App – e.g. commercial Apps, faxes, generic email etc.
- Individuals should be informed about the use of Pando via communication directly from their clinician and via privacy notices. This is the responsibility of the data controller. Clinicians must use the Pando App as directed by the IG teams within their individual Trusts and adhere to the good practice embedded into the end user agreement.
- Good practice in terms of data quality and minimisation is achieved via training and awareness and data resides on UK servers.
- The Forward Clinical Ltd / Pando development team are fully versed in the principles of 'privacy by design and default'.

Step 5: Identify and assess risks

Included below is a summary of the key privacy risks and impacts as related to the use of Pando. At all times Forward Clinical Ltd maintain an up to date information assets register, information security risk assessment and Hazards Log in compliance with SCCI0129.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation/corporate risk
Staff mobile devices lost or stolen	Confidential PID made public and/or vulnerable individuals targeted by criminals.	Confidential PID made public and/or vulnerable individuals targeted by criminals.	Confidential PID made public and/or vulnerable individuals targeted by criminals.
PID digital records intercepted over internet connections	As above	As above	As above
PID digital records stolen from server platform	As above	As above	As above

Step 6: Identify measures to reduce risk

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Staff mobile devices lost or stolen – subset of PID digital records no longer secured	(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.	(1) Risk significantly reduced (2) Risk reduced (3) Risk significantly reduced	Solutions are justified, compliant and proportionate responses to the aims of the project.
PID digital records intercepted over internet connections	(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.	(2) Risk significantly reduced (3) Risk significantly reduced	Solutions are justified, compliant and proportionate responses to the aims of the project.

PID digital records stolen from server platform	(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 password enforcement (security policy) and AES-256 server data encryption. (3) Regular penetration testing carried out for both servers and smartphone application.	(1) Risk eliminated (2) Risk significantly reduced	Solutions are justified, compliant and proportionate responses to the aims of the project.

Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By
Staff mobile devices lost or stolen	(1) All data encrypted at rest and in transit. No images, tasks, patient details stored on the device. (2) PIN code lock-down of all mobile devices is mandatory. (3) Remote Wipe function is included in Exchange/ActiveSync environments, free on iOS/Android and EMM (Enterprise Mobile Management) from Trust may be deployed.	CEO PM HoI DPO

PID digital records intercepted over internet connections	(1) Server Side Encryption (SSE), using 256-bit Advanced Encryption Standard (256-bit AES) in transit and at rest.	CEO PM HoI DPO

	(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.	
PID digital records stolen from server platform	(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 password enforcement (security policy) and AES-256 file-level server data encryption.	CEO PM HoI DPO

Ongoing Review: Integrate the DPIA outcomes back into the project plan.

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
(1) All data encrypted at rest and in transit. No images, tasks, patient details stored on the device. (2) PIN code lock-down of all mobile devices is mandatory. (3) Remote Wipe function is included in Exchange/ActiveSync environments, free on iOS/Android and EMM (Enterprise Mobile Management) from Trust may be deployed.	Actions completed by Forward Clinical Ltd.	CEO PM HoI DPO
Optional remote wipe function (Trust’s EMM – Enterprise Mobile Management) enabled and tested on higher-risk end-user devices.	To be confirmed with NHS Trust. Remote closing of account available via Pando	

	dashboard, 24/7 support available.	
(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, ensuring high levels of encryption. To further enhance security - OWASP certificate pinning implemented and access to Pando servers is only possible via SSH keys. (3) Strong Password policy enforced.	Actions completed by Forward Clinical Ltd.	CEO PM
(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 password enforcement (security policy) and AES-256 file-level server data encryption.	Most recent penetration testing of both application and entire infrastructure completed 9.4.18.	CEO PM

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 (see notes).**

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 a short-lived 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 a short-lived 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 a short-lived 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 a short-lived 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 a short-lived 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.**

Contact point for future IG/ data protection/information security concerns

Measures approved by Data Protection Officer dpo@hellopando.com

Last review July 2021 following DSP Toolkit submission.