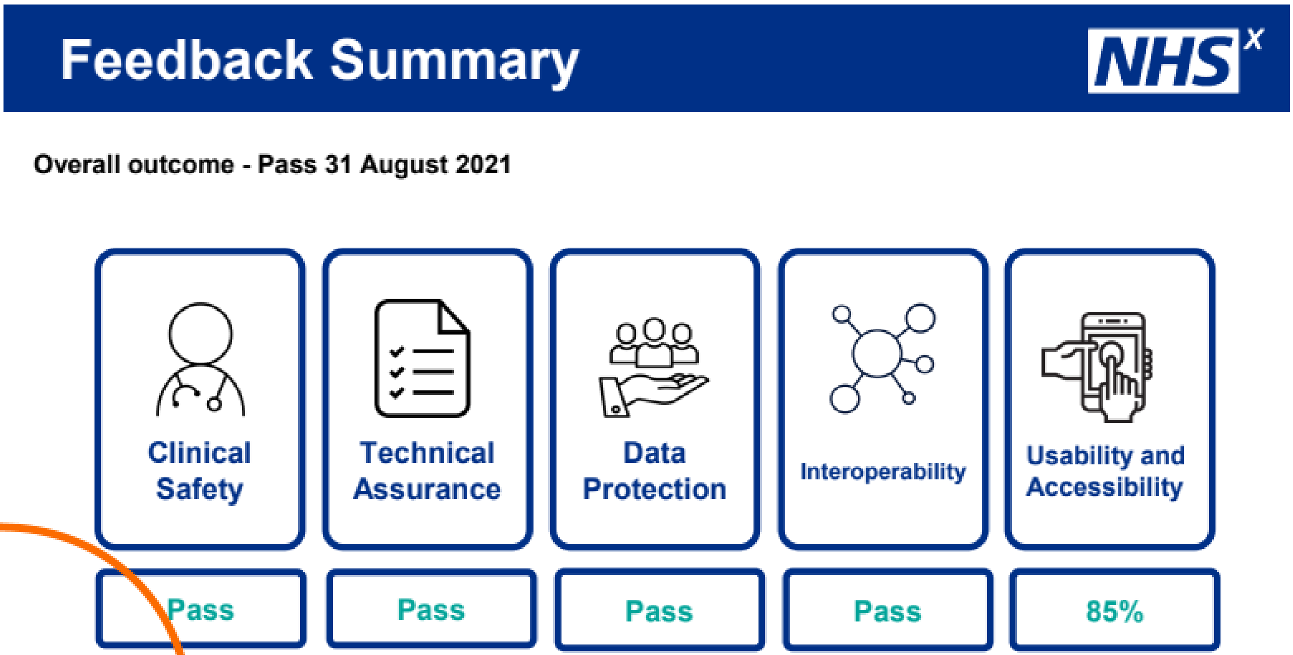
Pando Information Governance FAQ

The Pando App - A – Z of Data Protection and Security



Feedback Summary

NHSX

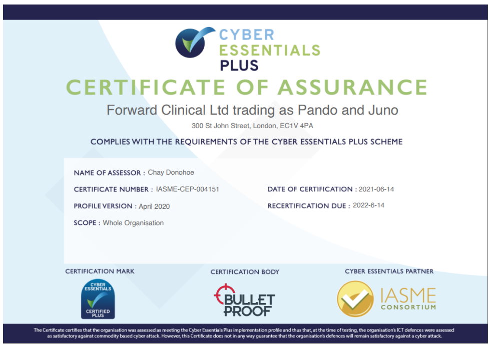
Overall outcome - Pass 31 August 2021

Clinical Safety	Technical Assurance	Data Protection	Interoperability	Usability and Accessibility
Pass	Pass	Pass	Pass	85%

How does i
working re

Accountability	The data controller (the community using Pando) is responsible for demonstrating compliance with the UK Data Protection Act/GDPR's data protection principles and must, therefore, ensure that any data processors (e.g. Forward Clinical Ltd who develop the Pando App) have measures in place to enable compliance with the data protection laws. If there is a breach, however, both the data controller and data processor are liable.	Accountability describes who is liable and responsible for complying with the UK's data protection laws. This is the Community using Pando and its employees as the controller and Forward Clinical Ltd who develop Pando as the processor.
Approved by NHS Digital (DTAC compliant)	The Pando App is officially approved by NHS Digital having undergone a rigorous DTAC evaluation process that examined the areas listed to the right in August 2021.	● Clinical safety - pass ● Technical Assurance - pass ● Data Protection - pass ● Interoperability - pass ● Usability and accessibility – 85%
Breach	A data breach is described by the GDPR as a breach of security that leads to destruction, loss, alteration, unauthorised disclosure of, or access to personal data.	Pando has been engineered to be secure by design and default in line with GDPR requirements. Forward Clinical Ltd is fully aware of its obligation to report any breach to the ICO within the 72-hour reporting window.
Data Controller	The person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.	The data controller is whoever controls how, why, and where personal information is used. In our scenario, the Community using Pando is the controller of message data created by its users and Forward Clinical Ltd is the controller of the data that relates to Pando App logins.

Data Flow Mappings	A ‘data flow map’ shows the ’flow ‘of an organisation's data and information from one location to another, e.g. from suppliers and sub-suppliers through to customers. When mapping data flows, the interaction points between all parties should be identified	The data flow mappings for the Pando application are included in graphical and tabular format in pages 9-12 of this document. Both can be included in your own data protection impact assessment.
Data Privacy Impact Assessment DPIA	Data protection impact assessments (DPIAs) help organisations to identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy.	Pando’s DPIA is kept under continual review. The latest version is always published on our website. We have a template to assist organisations to conduct their own DPIAs and our Data Protection Officer is on hand to answer any questions.
Data Processor	Anyone who processes personal data on behalf of a data controller.	This means that Forward Clinical Ltd processes the data within the Pando App based on the written instructions provided by the Community using Pando detailed in the signed data processing agreement.
Data Protection Authority	The national authority who protects data privacy. In the UK, this is the Office of the Information Commissioner.	We know this as the ICO.
Data Processing Agreement	A data processing agreement (DPA) is a legally binding document to be entered into between the controller (the Community using Pando) and the processor (Forward Clinical Ltd) in writing or in electronic form. It regulates the particularities of data processing – such as its scope and purpose – as well as the relationship between the controller and the processor.	Forward Clinical Ltd, (as the processor) will work with the Community using Pando (as controller) to ensure that both parties are meeting our Article 28 and 32 obligations.

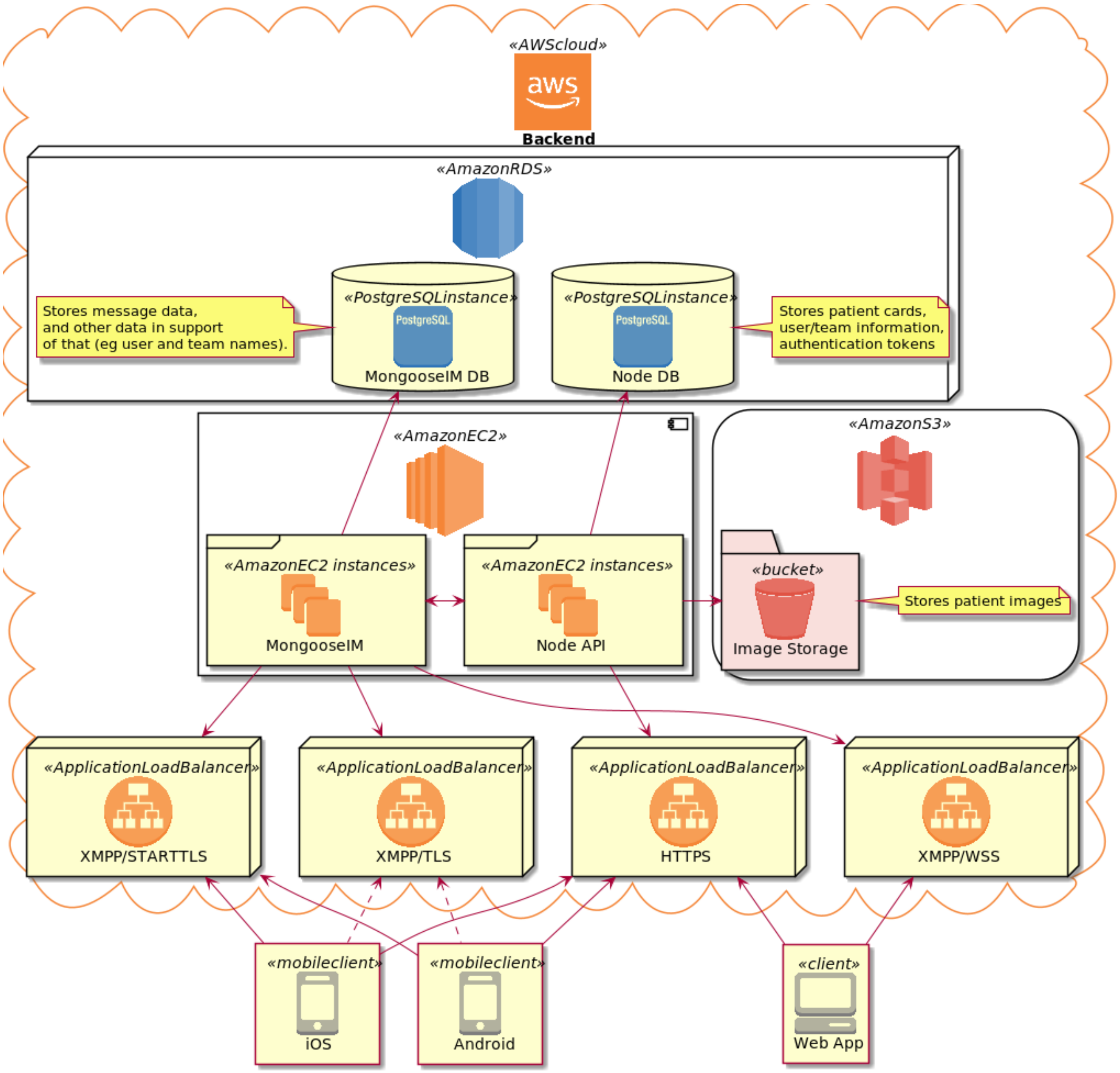
Data Protection Officer (DPO)	The DPO is tasked with formal responsibility for data protection compliance within an organisation. The appointment of a DPO under the GDPR is made mandatory when the organisation is a public authority or body.	Forward Clinical Ltd (Pando) has appointed a Data Protection Officer to ensure that personal information is kept safe and processed legally. The DPO can be contacted at dpo@hellopando.com
Data Subject	Someone whose personal data is processed by a Controller or Processor.	This is the person whose data is being processed (citizen, patient, or member of staff). They are any living person who can be identified by their personal data.
DSP Toolkit	Forward Clinical Ltd submitted DSP Toolkit to the NHS in June 2021 to the level of standards exceeded - https://www.dsptoolkit.nhs.uk/OrganisationSearch/8JP98	We are also Cyber Essentials Plus certified.  CYBER ESSENTIALS PLUS CERTIFICATE OF ASSURANCE Forward Clinical Ltd trading as Pando and Juno 300 St John Street, London, EC1V 4PA COMPLIES WITH THE REQUIREMENTS OF THE CYBER ESSENTIALS PLUS SCHEME NAME OF ASSESSOR : Chay Donohoe CERTIFICATE NUMBER : IASME-CEP-004151 DATE OF CERTIFICATION : 2021-06-14 PROFILE VERSION : April 2020 RECERTIFICATION DUE : 2022-6-14 SCOPE : Whole Organisation CERTIFICATION MARK CERTIFICATION BODY CYBER ESSENTIALS PARTNER The Certificate certifies that the organisation was assessed as meeting the Cyber Essentials Plus implementation profile and thus that, at the time of testing, the organisation's ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisation's defences will remain satisfactory against a cyber attack.
Encryption	Data, or plain text, is encrypted with an encryption algorithm and an encryption key. The process results in ciphertext, which only can be viewed in its original form if it is decrypted with the correct key.	Encrypted data is more secure than information which is simply stored in its original format. Pando's data is encrypted in transit & transferred via the HTTPS (SSL/TLS) protocol. Data is stored at a UK based data centre hosted by AWS & compliant with all relevant ISO standards (ISO27001).
Legal Processing	For any personal data processing, the organisation must be able to specify that it has been processed on one of the following legal grounds: The individual gives their consent. There is a contract with the individual (including pre-contract arrangements). Complying with a legal obligation.	Patient data is considered to be a special category of data under the UK GDPR and is processed under section 6(1)(c) "necessary for compliance with a legal obligation to which the controller is subject" and 9(2)(h) "(h) processing is necessary for the purposes of preventive or occupational medicine …

	If it is in the vital interest of the data subject. It is necessary for a task in public interest or authority. It is necessary in the legitimate interest of an organisation or third party (balanced against the interests of the data subject).	
Minimisation	You can only collect personal data that is needed to achieve an intended purpose. Personal data should be relevant and limited to what is necessary. Such data should also be updated when necessary.	Pando's Acceptable Use Agreement (AUP) agreement advises users to only collect and process the personal information that is needed.
On boarding and Off boarding	This refers to the process by which users are signed up to the Pando App in the first instance then removed from the system when they leave their position or move to a new organisation or Community.	We work proactively with all our clients. It is important that we discuss and agree the sensitivity of the data being processed and identify the appropriate technical and organisational measures that need to be in place. We refer to Article 32, which recommends that the Controller and the Processor shall implement technical and organisational measures required. In this respect: 1) Any leavers' accounts are disabled. 2) Account list is reviewed on at least once a year as per a pre-established schedule 3) Where technically feasible, a user account not used for a period of 45 consecutive days is disabled.
Photographic Images	Under GDPR, a photograph is deemed personal data. Clinicians and users of the Pando App should follow the IG guidelines of their employer in respect of clinical images.	Pando allows teams to edit and share images instantly, securely, and they can also be exported to NHS.net email.

Processing	This refers to any activity relating to personal data, from beginning to end. It includes the organising, altering, making use off, transferring, combining, holding and destruction of data, either electronically or manually.	Data processing means, everything you could think of that can be done with personal information. It includes the messages transmitted by Pando when they contain personal data – e.g. a patient's name.
Security by Design and Default	The ability to ensure the ongoing confidentiality, integrity, availability, and resilience when processing personal data, while also using appropriate technical, organisational and security measures.	Security is at the centre of our design and technical developments. We have built Pando in line with all DSP recommendations & regulations and it is officially approved by NHS Digital's DTAC evaluation. Pando meets all NHS & GMC standards on confidentiality.
Subject Access Request (SAR)	This right of subject access means that anyone can make a request under the Data Protection Act 2018 to any organisation processing their personal data. An individual can ask the organisation that they think is holding, using, or sharing the personal information to supply them with copies of both paper and computer records and related information.	In respect of access to patient information (SARs), Forward Clinical Ltd is always the data processor and the Community is always the controller. Pando's Acceptable Use Agreement (AUP) stipulates that all communications must be transcribed to the patient record as Pando is a communication portal, not a permanent healthcare record. Messages are held on encrypted drives and Pando has technical and organisational measures in place to ensure our own staff cannot get access to the messages. However, we can facilitate a Subject Access Request so long as we have a signed Data Processing Agreement in place but will only act upon the instructions of the data controller.

Subject Rights	The data subject has the right to: ● Transparency (to be informed). ● Access the data. ● Rectify the data. ● Request that the data be erased. ● Restrict processing. ● Data portability. ● Object to the processing of data. ● Not to be subject to a decision based solely on automated processing.	These are all the legal rights of an individual in relation to personal data. However, we recognise that not all of them will apply in all circumstances. For example, a patient could not simply ask for their health record to be erased.
Transparency	Under the accountability principle laid out in Article 5.2, a data controller "must be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject." These transparency obligations begin at the data collection stage and apply "throughout the life cycle of processing." Pando's Privacy Policy is available here. https://hellopando.com/privacy-policy/ If you would like any further information or would like to discuss this further, please contact dpo@hellopando.com	We advise that an organisation that uses Pando should ensure that patients are made aware of this by way of a privacy notice on their website and patient leaflets. They can also cross reference to the Pando privacy policy in the Privacy Centre. Pando is a secure shared messaging system that allows staff within the Community to communicate efficiently and safely about patients, to deliver the best possible care and improve efficiency. As stated in Pando's Acceptable Use Policy, the App does not replace patients' permanent healthcare records, which will always be updated in the usual way.

Data Flows and Security



General Security Model: Our Security Model is based on the primary attack vector being the mobile devices of our users. These are usually user owned and managed, and therefore often in public spaces. Therefore, our model minimises data stored by the app on the device and optimises for the case where the device is lost or stolen. Any data held on the device is therefore a minimal cache and can be destroyed without warning without clinical data loss.

User registration: Users must have access to a whitelisted domain email address to register with Pando. On entering that email address, an activation code is sent to the email address which must be entered to gain access to the app. This activation code remains active for 24 hours. Additionally, the NHS.Net SSO service can be used instead of an activation code.

PIN login: Users must set a 4-digit PIN which must be entered to gain access to the app. This PIN cannot be removed, and the timeout cannot be altered by the user. Users are also able to utilise mobile device biometric security if enabled by their device instead of the PIN.

User access to patient information: Pando does not provide a searchable patient database. Users can only gain access to patient information if they have entered that information into the app, or if invited to view a patient profile by another clinician.

Encryption in transit: In transit data is encrypted using the TLS protocol (for example, using HTTPS). When transmitting messages devices use a minimum of a TLS 1.2 handshake with 2048-bit RSA keys to encrypt the socket connection to our servers. We support the sync of RSA public keys. To further enhance security, we have implemented OWASP certificate pinning in a number of cases. All internal communication is also protected by TLS.

Encryption at rest: All data is held on Amazon Web Servers London Cluster and is encrypted at rest to a minimum AES-256 bit standard. AWS is compliant with numerous ISO standards including ISO 27001/2.

iOS Client: An authorisation token (used to authenticate to the servers) is held within the Keychain along with profile information about the user. A minimal cache of message data and images is stored on the device within the application’s encrypted enclave, which is only decrypted when the app is running, and is inaccessible to other applications.

Android Client: An authorisation token is stored within the “Shared Preferences” specific to the application. This, alongside imported photos, is stored within the application’s private directory and protected by Operating System restrictions. The token is also used to encrypt the local database holding the minimal message cache and cache of Gallery metadata.

Web App: The Web Application runs entirely within the Browser Sandbox and stores no permanent data locally. A token-based authentication system is used currently, as per mobile systems. An authentication cookie may be added to allow a persistent login.

Deletion from servers: Deletion from the database is automated to occur at five years. Data can be deleted manually before that time if necessary.

Access to servers: Access to servers is only via known SSH keys, via a bastion server firewalled to known IP addresses. All workstations used to access the servers conform to Cyber Essentials Plus.

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.**