Data Protection Impact Assessment (DPIA)

GPintheCloud service

Service Owners

Delt Shared Services Ltd	Giles Letheren	CEO/SIRO
Integy Ltd	James Cook	Joint Founder

Completed by	Giles Letheren	Date	13/5/2022

Overview

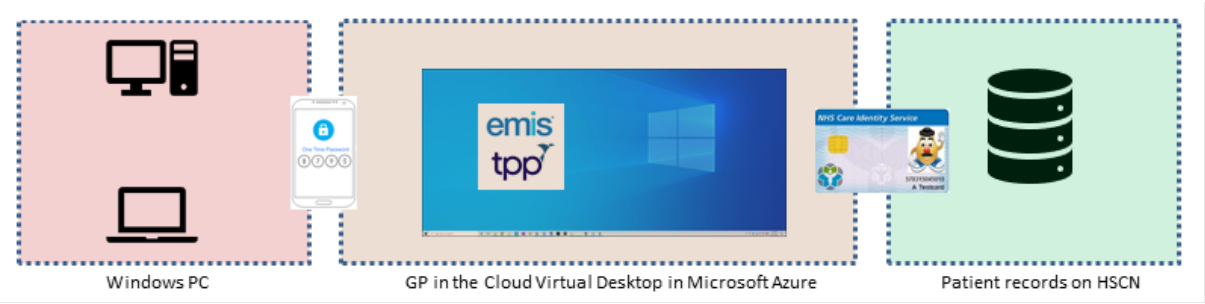
1. Background

GPintheCloud is a clinical remote desktop, designed to support Primary Care, developed by a joint venture partnership between Delt Shared Services Ltd and Integy Ltd.

GPintheCloud makes use of standard cloud computing components and connectivity to the HSCN to allow suitably authorised users connectivity to and use of primary care clinical systems and supporting applications.

It is important to note that access to clinical systems enabled by GPintheCloud uses existing access control lists (via an NHS smartcard) to manage rights to clinical data and these remain under the control of existing data controllers.

2. Data flow diagram



3. Purpose of the processing

This is a solution to provide a secure remote clinical desktop, accessible from any suitable internet connected device, to suitably authorised users.

GPintheCloud has been built for the needs of Primary Care and provides access to both SystmOne and EMIS Web clinical systems along with other supporting applications. Onward connectivity to other HSCN services including HSCN hosted pathology systems is provided, though access to individual services may be subject to additional security controls.

GPintheCloud was initially designed for use by remote locums, supporting general practice but there are several other suitable use cases:

- Practice business continuity, including support staff
- Provision of primary care system access to authorised pharmacy users
- Provision of primary care system access to authorised medical examiners

Description of the processing

4. Nature and scope of the processing

GPintheCloud provides access to both SystmOne and EMIS Web clinical systems along with other supporting applications. Onward connectivity to other HSCN services including hosted pathology systems is provided. Whilst the service allows access to patient records it does not control access to patient records and clinical systems themselves, this remains under the control of the applicable data owner.

GPintheCloud is available to CCGs/ICSs. It is not presently available to other organisations.

5. Data Processed

5.1 To provision access to the GPintheCloud service

Delt Shared Services Ltd and Integy Ltd are joint controllers for this data processing

- Users name
- Users GPintheCloud Account ID or N365 ID
- Users' password hash
- Users email address
- Users phone number
- Users' authorisation status* (active/inactive)

5.2 To manage the GPintheCloud service

This data is used for accounting and security monitoring.

Delt Shared Services Ltd and Integy Ltd are joint controllers for this data processing

- Users GPintheCloud Account ID or N365 ID
- Times of Access and services consumed
- Source IP Address
- Geo-Location data sourced from IP address

Of this data the last 90 days of:

- GPintheCloud Account ID or N365 ID and
- Times of Access and services consumed

May be shared with CCGs/ICSs who authorised the clinician as a user of GPintheCloud.

5.3 To support access to the GPintheCloud service

Delt Shared Services Ltd and Integy Ltd are joint controllers for this data processing

- User's account information as listed above
- Contact made by GPintheCloud service users, made by email, instant message, or phone.
- Support calls may be stored as an audio recording

Delt Shared Services Ltd and Integy Limited will use Microsoft as a data processor for provision of the virtual desktops and management information related to the service.

Delt Shared Services Ltd will use ServiceNow as a data processor for incident management, and Avaya for support desk telephony.

Integy Ltd will use ConnectWise as a data processor for incident management.

This data will be managed in line with the respective organisations' existing IT support processes.

5.4 With respect to patient data

For the purposes of data protection law terminology, Delt Shared Services Ltd will be the data processor and Integy Ltd will be the data sub-processor.

This includes:

- The 'window' into clinical systems to which the user has been authorised by the employer or Practice who are the data controller
- Any temporary files created by the clinician whilst using the VM for the duration of its lifespan (not more than 30 days). It is therefore not recommended that clinicians use this functionality to create content outside of the clinical systems, the customer organisation is however responsible for directing their clinicians in use of the service.

This therefore comprises any and all personal data types which the clinical systems enable access to, both patient and clinical system users (for example information recorded by the clinical system when a patient record is updated), and those special category personal data types this includes.

This access remains under the control and gift of the data controller of the clinical system data (for example, the Practice the user is providing services to).

Application of Data Protection Principles

6. Lawful basis

Provision of a service to enable individuals identified by CCGs/ICSs as requiring access to the clinical desktop in order to perform work for which they are or will be contracted.

Data which is part of the clinical system remains part of the applicable data controller's existing data arrangements, and is for them to determine the appropriate lawful basis

The lawful basis for processing data in relation to the GPintheCloud service is Legitimate Interest. A Legitimate Interest Test has been completed to validate this conclusion

7. Demonstrate the fairness of the processing

For authorised users to access GPintheCloud, a CCG/ICS will have requested they are specifically set up as a user.

The user will also be aware they are accessing a system as they will be logging in. Users would expect usage to be captured at a system level (such as capacity management), and at a local level (such as for support issues).

Data which is part of the clinical system remains part of the data controller's existing data arrangements, however, patients would expect that clinicians can access their patient record.

8. What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?

A transparency notice is provided on the GPintheCloud support website, which is referenced in all communication with end users, including initial setup documentation. This notice explains what data is processed and why and informs data subjects of their rights and

methods for resolving any issues. The location of the transparency notice will also be signposted to users in the GPintheCloud log on message.

Data which is part of the clinical system remains part of the data controller's existing data arrangements. There is no change to usage of patient data or clinical employee data, just an additional way for an authorised user to access existing applications.

9. Is it necessary to collect and process all data items?

Data identifying GPintheCloud users will be limited to that which is required to manage their account.

This list describes the purpose of data processed relating to the users of the GPintheCloud system. Data which is part of the clinical system remains part of the data controller's existing data arrangements.

Personal Data

Data Processed	Purpose
Users name	Communicating with the authorised user
Users GPintheCloud Account ID or N365 ID	Managing access to GPintheCloud
Users' password hash	Managing access to GPintheCloud
Users email address	Communicating with the authorised user
Users phone number	Communicating with the authorised user
Users' authorisation status* (active/inactive)	Managing access to GPintheCloud
Details of any support contacts	Managing resolution of incidents and to ensure contact quality
Times of Access and services consumed	Managing billing for service consumption. Access management
Source IP Address	Access management. Cyber security monitoring
Geo-Location data	Access management (inferred from IP address so may be inaccurate)

Special Category Data

None

10. How will you ensure data is not used for other purposes?

As documented in the Joint Venture Agreement, neither Delt Shared Services Ltd nor Integy Ltd will use data processed as part of the GPintheCloud service for any other purpose.

Data which is part of the clinical system remains part of the applicable data controller's existing data arrangements.

11. How will you ensure the accuracy of the data?

The personal data collected will either:

- be supplied by a CCG/ICS in order to enable authorised user access and if incorrect will be evident to the user within their account credentials, which they can contact GPintheCloud support to correct; or
- in the case of usage data, be captured automatically by proven, industry standard logging tools.

Data which is part of the clinical system remains part of the applicable data controller's existing data arrangements.

12. How long will the personal data be kept for?

Data identifying GPintheCloud users (5.1) will be automatically deleted 90 days after the account is deauthorised by an administrator.

User access data (logs) will be maintained for 90 days, after which they will be deleted.

User data (username, access credentials, contact details) is maintained for the period of authorisation. The commissioning body (CCG/ICS) will be asked to validate this list at least once every 24 months.

Any data cached by the applications delivered via GPintheCloud is deleted when the virtual machine session is terminated, which is no more than 30 days.

Information may be included as part of records relating to support activities such as fault finding and resolution. In this case it will be kept for the lifecycle of the support products.

Data which is part of the clinical system remains part of the applicable data controller's existing data arrangements and is not affected by this solution.

13. What technical and organisational controls for information security have been put in place?

13.1 GPintheCloud

- Multifactor authentication is used to secure access to GPintheCloud
- Virtual machine machines storage is encrypted at rest.
- Traffic between the user and GPintheCloud is encrypted.
- A Systems Level Security Policy (SLSP) is in place.
- GPintheCloud has been subject to a third-party penetration test with all recommendations applied. *NB: This is pending completion of the build but will be completed prior to launch.*
- Virtual machines are built from a standard image, so can easily be destroyed, and recreated and data persist only for the life of the machine (no more than 30 days).
- Virtual machines will be replaced every 30 days, ensuring
- Internet access filtering is in place to ensure that outbound web browser access cannot access undesirable classifications of websites.
- GPintheCloud will timeout after 10 minutes of inactivity after which a user will be required to reauthenticate – there will be no loss of data in this scenario.
- A session with no activity for 60 minutes automatically logs out – in this scenario any unsaved data would be lost.
- A reminder of the conditions for using GPintheCloud is presented on each logon, including the condition that photographs of screen displays may not be taken.

- A Joint Controller agreement details respective responsibilities of Delt Shared Services Ltd and Integy Ltd, which includes a sub-processing agreement.
- Screen Scrape Protection
- Microsoft Baseline Security Policies
- NCSC Approved UK Official / NHS Azure Policies
- Written training material is provided to all GPitC users, with the option of telephone support
- Both Delt and Integy staff are subject to pre-employment checks including DBS checks where appropriate
- Both Delt and Integy staff are provided with formal Data Protection and cyber security training
- Both Delt and Integy staff responsible for the management of the GPitC platform will receive training appropriate to their role
- Changes to the service are managed under a formal change control process as part of the System Security Policy. This document is available for customers to review under an appropriate NDA.
- In the unlikely event of a data loss incident, Delt will manage the process against its standard procedure.

13.2 Clinical systems data

It is the CCG/ICS's responsibility to request a GPintheCloud account is deauthorised. However, without access granted by the data controller of the clinical system (e.g., the Practice) GPintheCloud will not, on its own, enable access to clinical data.

Data which is part of the clinical system remains part of the data controller's existing data arrangements, and existing smartcard functionality is required to access clinical applications themselves.

The Joint Controller agreement referenced above (13.1) also includes processor to sub-processor requirements where Delt Shared Services Ltd and Integy Ltd in the processing of clinical systems data

Data Sharing

14. Describe if the personal data is to be shared with other organisations and the arrangements you have in place

User and usage data will be shared with Microsoft Ltd, a technology provider to GPintheCloud.

Usage reports will be available to CCGs/ICSs for their own authorised users only.

Patient data will not be shared as a consequence of GPintheCloud usage. Data which is part of the clinical system remains part of the applicable data controller's existing data arrangements.

Data Matching

15. Describe if personal datasets are to be matched, combined, or linked with other datasets (internally or for external customers)

Neither user nor patient data will be matched, combined, or linked with other datasets as a consequence of GPintheCloud usage.

IP address data and login information may be matched with other datasets in the interests of ensuring cyber security.

Data Subject Rights

16. Describe how data subjects will be able to exercise rights granted by data protection legislation

GPintheCloud data subject may contact Delt's DPO as a point of contact. Contact information will be included in the Transparency Notice published on the GPintheCloud website.

Any requests for correction/objection will be processed through the Delt Service Desk, or the organisation who receives them.

Any requests for access will be managed and monitored using Delt's Subject Access Request process

Clinical system data subjects will remain covered by the applicable data controller's existing arrangements.

Geographical Location

17. In which country/territory will personal data be stored or processed?

All clinical data will remain within the UK.

User and usage data for GPintheCloud may be stored in the UK and US (the later has Standard Contractual Clauses in place).

Risk Register

Ref	Describe the source of risk and nature of potential impact on individuals.	Probability	Impact	Overall risk	Mitigation	Probability	Impact	Residual risk rating	Measure approved
	Include associated compliance and corporate risks, as necessary.	*1-5*	*1-5*	*Probability x Impact*		*1-5*	*1-5*	*Probability x Impact*	*Back office only*
1	Personal data (limited to names and email addresses of users) is leaked or stolen from within GPitC platform	2	3	6	Apply Azure baseline security policies. Secure with MFA. Penetration test. Minimisation of dataset. Data encryption.	1	3	3	
2	Provisioning of an internet accessible route to patient data increases the security risk to that data	2	5	10	Secure with MFA. Penetration test. Access to patient data also requires authorised NHS Smartcard. Data encryption.	1	5	5	
3	Theft or unauthorised use of written down credentials, users' mobile phone and smartcard would allow unauthorised access	2	5	10	Remind users not to write down access credentials and store secure access technologies (like smart cards) separately from devices	1	5	5	

4	Third party view of patient data on a screen	3	5	15	Clinicians are bound by local standard contractual terms and NDA's. Clinicians reminded of the risks of working in public view.	2	5	10	
5	Inappropriate use	1	5	5	Clinicians are bound by local standard contractual terms and NDA's.	1	5	5	
6	Authorised users take photos of patient data	2	5	10	Screen shot functionality disabled. Pop up reminder on each login that doing so using a camera is a breach of terms and conditions	1	5	5	
7	Inappropriate users gain patient records access	1	5	5	Authorised users are identified by CCGs/ICSs. In the unlikely event of an unauthorised user being granted GPitC access, there would be no access to patient data without a smartcard authorised by an individual GP Practice.	1	5	5	
8	Lack of availability GPintheCloud of (Azure failure, DOS attack, data corruption)	1	3	3	None required. The underlying GPintheCloud infrastructure is highly resilient. GPintheCloud is not a critical service but a	1	3	3	

					secondary access mechanism.				
9	The service is impacted by the end of the partnership between Delt Shared Services Ltd and Integy Limited.	3	3	9	End of partnership arrangements are documented in the Joint Venture Agreement.	3	1	3	
10.	Risk that GPintheCloud users may not be aware that their information is being processed in this way which would result in a failure to adhere to the transparency principle and Article 13 and 14 under the UK GDPR.	2	1	2	Transparency Notice will be published on the GPintheCloud website, signposted to subscribing organisations	1	1	1	

See table below for guide to assessing risk

Probability	Rating	Impact	Rating
1 - Rare	1	1 - Insignificant (Low - no business impact)	1
2 - Unlikely	2	2 - Minor (low - minor business impact, some loss of confidence)	2
3 - Moderate	3	3 - Moderate (medium - business is interrupted, loss of confidence)	3
4 - Likely	4	4 - Major (high, business is disrupted, major loss of confidence)	4

5 - Almost Certain	5	5 - Catastrophic (high - business cannot continue)	5

Calculating Overall Risk and Risk Rating

Score	Rating	Action
15-25	High	Immediate action required to mitigate the risk or decide not to proceed
5-14	Medium	Action should be taken to compensate for the risk
1-4	Low	Risk should be monitored and tolerated

DPO Advice

DPO/SIRO advice provided
It is recommended that the project should Ensure the following actions are completed: • All technical and organisational controls listed in this DPIA • Completion and publication of Transparency Notice on GPintheCloud website • Update to log in screen to include signposting to Transparency Notice on GPintheCloud website • System Security Policy (including change control process arrangements) • Completion and signing of the Joint Controller agreement laying out roles and responsibilities and including a standard Processor to Sub-processor agreement between Delt and Integy relating to the clinical data which GPintheCloud processes. • Completion of the Legitimate Interest Test form At the point at which the design of the live service is finalised: • review the DPIA and all supporting service documentation, including but not exclusive to documentation provided to customer organisations and data subjects, to ensure they are accurate and complete. • Joint controllers should consider how both parties will be kept up to date with the most current reference information relating to this service as part of the joint venture. As new data controllers are brought on board • Ensure that any Data Processing Agreements signed between Delt, and any Data Controllers reflect the terms laid out in the appendix of the Joint Controllers agreement which also sets the Processor to sub-processor agreement between Delt and Integy for the clinical data made accessible by the GPintheCloud service and take appropriate action if not. This DPIA should be revisited if changes are made to the service/the expected service to ensure accuracy and completeness and should be resubmitted for review if updates are made.

Name	Kate Joy
Date	16th May 2022