Data Protection Impact Assessment – NHS.net Connect (formerly NHSmail) Unattended Robotic Process Automation (RPA)

Document filename:	**Data Protection Impact Assessment**	
Directorate / Programme		NHS.net Connect
Document Reference *[insert IAR reference number]*		
Information Asset Owner	*John McGhie*	Version 1.0
Author	*NHS.net Connect team*	Version issue date *September 2025*

Document Management

Revision History

Version	Date	Summary of Changes

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Jessica Davenport	Service Manager	17 Sept 2025	1.0

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
John McGhie	Head of Collaboration Services	Sept 2025	1.0

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help NHS England demonstrate how we comply with data protection law.

DPIAs are also a legal requirement where the processing of personal data is *"likely to result in a high risk to the rights and freedoms of individuals".* If you are unsure whether a DPIA is necessary, you should complete a DPIA screening questionnaire to assess whether the processing you are carrying out is regarded as high risk.

By completing a DPIA you can systematically analyse your processing to demonstrate how you will comply with data protection law and in doing so identify and minimise data protection risks.

This document should be read in conjunction with the DPIA Guidance and DPIA Screening Questionnaire

1. Consultation with Stakeholders

This DPIA covers the capability to enable Unattended Robotic Process Automation (RPA) using Power Automate on Windows 365 Cloud PCs or locally provisioned Virtual Machines and will be applicable to any local organisation and individuals choosing to deploy Unattended RPA workflows.

The following stakeholders were engaged for input / review of the DPIA:

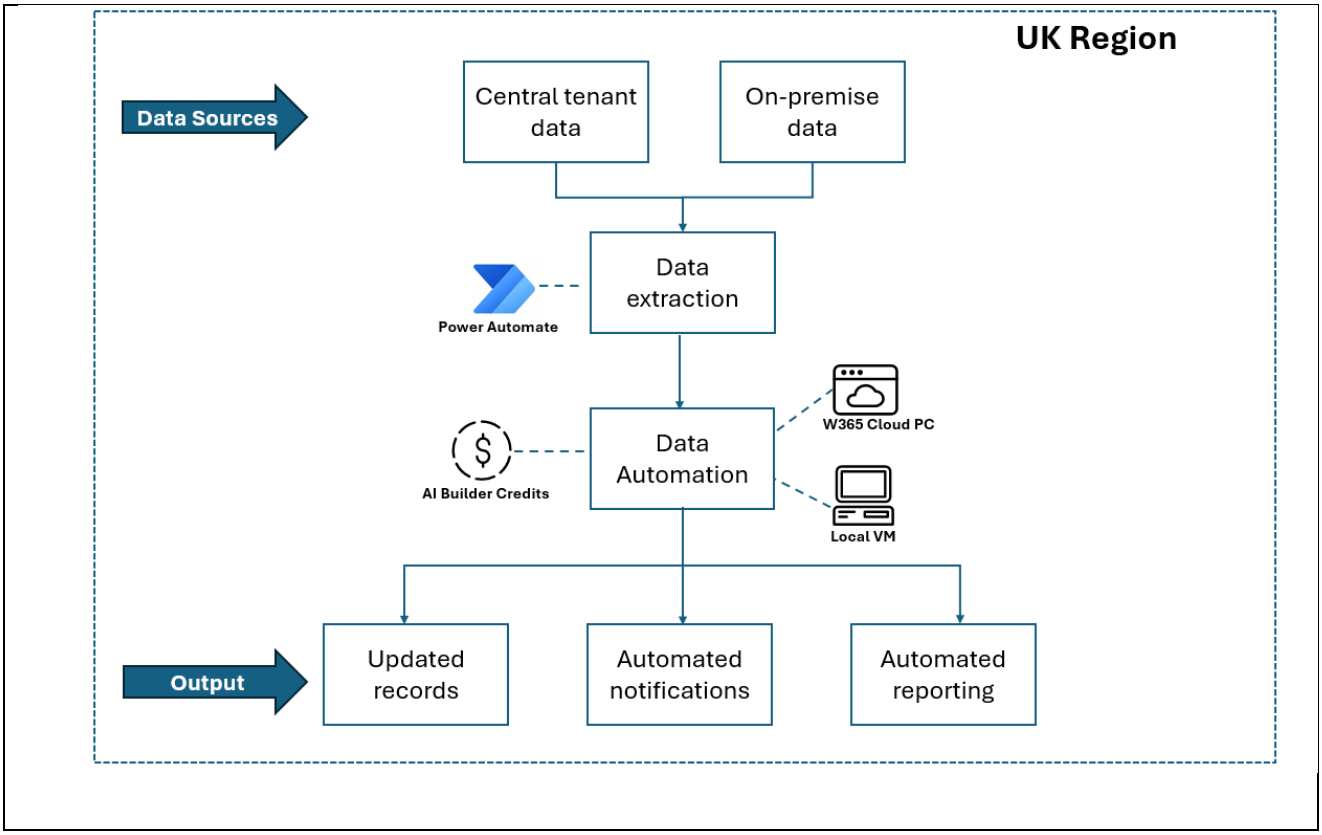
- NHS.net Connect programme leads - including service owners, SIRO, technical, solution assurance, IG and security leads and Clinical Safety Officer
- Accenture programme leads - including service owners, technical, IG and Security leads and Clinical Safety Officer

2. Data Flow Diagram

Unattended RPA enables automated execution of desktop flows without human intervention, improving efficiency and streamlining repetitive tasks.

While the capability to enable Unattended RPA is available within the NHS.net Connect tenant, the development of the workflows will be the responsibility of the local organisations and will depend on the specific use cases.

This diagram illustrates how data flows in Power Automate. Please note that this can vary, the diagram shows example use cases:



3. Purpose of the processing

The capability for Unattended RPA is enabled and provided within the NHS.net Connect tenant to support the deployment and automated execution of workflows.

The specific use cases for Unattended RPA will depend upon the workflows defined by local organisations and as such the responsibility for defining the purpose of the processing will be with the local organisation and should be documented within a supporting DPIA, if personal data is to be processed.

Local organisations should also consider the impact of any automated decision making and profiling regarding individuals - Automated decision-making and profiling | ICO

4. Description of the Processing

Nature and scope of the processing:

NHS.net Connect is encrypted to a secure standard to allow document classifications of OFFICIAL (including the subset OFFICIAL SENSITIVE) to be stored and communicated, however NHS.net Connect should not be used as a replacement to any Patient Record System (but can be used in conjunction with, depending on local policies).

The existing data controller and processor arrangements are outlined in the published: NHS.net Connect Data Protection Impact Assessment - ENGLAND – Data Protection Impact Assessment – NHS.net Connect Support

And

ENGLAND – NHS.net Connect UK GDPR Joint Data Controller Table – NHS.net Connect Support

Use of Unattended RPA does not make any changes to existing UK GDPR roles and responsibility arrangements to NHS.net Connect organisations, within the tenant.

NHS England and each organisation that are part of the pilot are Joint Data Controllers for their respective roles:

- NHS England are the Data Controller for service configuration and provision.
- Each organisation on the tenancy is Data Controller for the data they enter into NHS.net Connect.
- Accenture is Data Processor acting upon instruction from NHS England and Microsoft are Sub-Data Processor.

All records will be electronic.

Organisations will be responsible for the creation and management of DPIAs specific to the Unattended RPA use cases deployed for their organisation.

Description of processing:

No data will be processed by the establishment of the Unattended RPA capability. However, it's implementation and adoption by organisations and individuals will involve the processing of data because of the use cases they create. Data processing is required to enable the automated execution of processes without human intervention. The data processed could include personal data.

Context of the processing (roles and responsibilities):

Organisations will be responsible for ensuring a specific Data Protection Impact Assessment (DPIA) is completed before Unattended RPA flows are deployed, as necessary.

All Unattended RPA flows should be tested sufficiently, and NHS organisations remain responsible for ensuring that all RPA-driven workflows undergo appropriate assessment. Unattended RPA is not intended for clinical use in its default configuration and the

associated clinical safety activities have NOT been completed by NHSE. Organisations wishing to deploy Unattended RPA-driven workflows in a clinical context must complete the necessary governance and clinical assurance processes, **including the production of a DCB0160**-compliant Clinical Safety Case Report and Hazard Log.

Organisations wishing to deploy automated workflows involving systems containing medical data must assess, define and manage the associated risks for such use cases and ensure that these use cases are included within a DPIA.

Local organisations remain responsible for ensuring their Unattended RPA users and flows are compliant and licensed appropriately.

5. Describe the legal basis for the processing (collection, analysis or disclosure) of personal data?

Legal basis for collection and analysis: NHS.net Connect covered by direction issued by the Secretary of State for Health and Social Care where NHS England is appointed as the Service Provider for NHS.net Connect, taking responsibility for setting up and managing the data processing contract for the service on behalf of all Controllers.

Health and Social Care Act 2012 – Direction:

Informatics systems for the collection or analysis of information Directions 2016 - NHS England Digital

Local organisations are required to establish their own legal basis as outlined in the **ENGLAND – NHSmail UK GDPR Joint Data Controller Table – NHSmail Support.**

Legal basis for disclosure:

N/A

6. Demonstrate the fairness of the processing

Data processing by NHS England and Accenture to run and maintain NHS.net Connect

The NHS England Transparency / Fair Processing document has been produced to confirm how NHS.net Connect meets the UK GDPR duty of transparency. NHS.net Connect has an Acceptable Use Policy (AUP) which staff (NHS.net Connect users) are required to read and accept before using NHS.net Connect. The AUP sets out the way the

service runs, how users are expected to behave, and the data retention periods for data stored about them and the data that they send and receive via NHS.net Connect.

Local organisations using NHS.net Connect are required to ensure their staff (NHS.net Connect users) have read and understood the policy documents and guidance provided by the NHS.net Connect Service. The Transparency / Fair Processing Information sets out how NHS.net Connect complies with UK GDPR and should be used by NHS.net Connect users in conjunction with the Transparency / Fair Processing Information provided by their local organisations (as Joint Controllers).

Only data which is included within the defined scope of the Unattended RPA will be processed. Local organisations must consider the fairness of their use case for each Unattended RPA configuration and must follow local organisational policies when inputting personal, sensitive or clinical data relating to any other individuals, including ensuring that they have adequate permission to process the data.

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

Organisations will be responsible for informing individuals about the ways in which their personal data may be used depending on the scope of the developed and deployed Unattended RPA workflows.

A user guide has also been established to provide an overview of the Unattended RPA capability.

Useful links:

ENGLAND – Transparency / Fair Processing Information – NHSmail Support

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

Data items outlined in the published Data Protection Impact Assessment are processed subject to local organisation need and processes and individual user needs.

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

No datasets will be matched, combined or linked with other datasets based on the existence of the Unattended RPA capability provided with the NHS.net Connect service. Organisations will be responsible for any applied use cases for Unattended RPA, including ensuring additional DPIAs are created when necessary.

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

No data sharing agreements with any other organisations exist based on the Unattended RPA capability provided with the NHS.net Connect service. Organisations will be responsible for any applied use cases for Unattended RPA, including ensuring additional DPIAs are created when necessary.

11. How long will the personal data be retained?

Any data that resides in M365, including personal data, is the responsibility of local organisations and is subject to local information governance. Local organisations must update transparency information to record how this data is captured and stored. Please see the retention period for Power Automate within the central tenant here Data Retention and Information Management Policy – Office 365 – NHSmail Support

12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date

Local organisations will be responsible for ensuring any personal data used within their Unattended RPA workflows is accurate and kept up to date.

13. How are individuals made aware of their rights and what processes do you have in place to manage such requests?

Individuals are informed of their rights within the Acceptable Use Policy and it will also be the responsibility of the organisation to ensure that individuals are informed as to the specific use cases implemented using Unattended RPA in their organisation.

Useful links:

ENGLAND – Transparency / Fair Processing Information – NHSmail Support

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

The existing technical and organisational controls for NHS.net Connect are in place for Unattended RPA, including the Identity and Access Management controls and authentication methods.

Controls which should be implemented by each organisation using Unattended RPA:

- **Implement Tenant-Level DLP Policies**: To ensure compliance with data regulations, organizations should request a 'Basic','Advanced' or 'Advanced + Unattended RPA' Data Loss Prevention (DLP) policy for their environments to restrict access to specific connectors. Please see DLP Policy – NHSmail Support for more information on NHS.net Connect DLP policies. It is crucial to classify the Desktop connector as 'Business' to prevent potential data leaks. Please see Connector classification - Power Platform | Microsoft Learn for more information on how connectors are classified. The DLP policy from the central Power Platform environment will apply to every Power Platform environment for each trust, providing a consistent level of data protection across the organization. for more information on how connectors are classified. The DLP policy from the central Power Platform environment will apply to every Power Platform environment for each trust, providing a consistent level of data protection across the organization.
- **Ensure Data Encryption**: Organizations must ensure that all data is encrypted by default and ensure to manage credentials securely, providing security both at rest and in transit. These measures will safeguard sensitive information, maintain data integrity, and create a secure and compliant unattended RPA environment. Please see About data encryption - Power Platform | Microsoft Learn to learn more about encrypting your data.
- **Manage Data Permissions**: Data permissions in Power Platform should be managed through security roles and the principle of least privilege, which define the actions users can perform and the data they can access. Organizations should create custom roles to meet specific needs and assign them to users, teams, or groups within environments. This approach ensures appropriate access levels,

ensuring the right people have access to data sources and outputs while maintaining data security and compliance. Please see more information on security roles here Security roles and privileges - Power Platform | Microsoft Learn

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

In Power Automate, your flows are created within your Microsoft Power Platform environment. These environments are specific to a region, which corresponds to the location of the data centres where your Microsoft Power Platform environment is stored. For the NHS.net Connect tenant, this is the UK, where the Microsoft Power Platform environments are stored. This helps ensure that data is managed efficiently and securely within the appropriate geographical boundaries and allowing compliance with data residency laws. Please see Regions overview for Power Automate - Power Automate | Microsoft Learn for information on region mapping and how environment admins can identify the region of their flows via the Power Platform admin centre. If a Local Admin does not have environment admin permissions they can raise a ticket with helpdesk to confirm the regions.

16. Does the National Data Opt Out apply to the processing?

N/A

17. Identify and assess risks

Consider the potential impact of your processing and the potential harm or damage that it might cause to individuals whether physical, emotional, moral, material or non-material e.g. inability to exercise rights; discrimination; loss of confidentiality; re-identification of pseudonymised data, etc.

You can also use this section to detail any risks you have in complying with data protection law and any resulting corporate risks e.g. impact of regulatory action; reputational damage; loss of public trust, etc.

The below potential risks are indicative and depend on the specific use cases implemented by local organisations and should be included with the additional DPIAs created to cover the deployed Unattended RPA use cases as appropriate.

Describe source of the risk and nature of potential impact on individuals	**Likelihood of harm** (Remote; reasonable possibility or more likely than not)	**Severity of impact** (Minimal impact; some impact; or serious harm	**Overall risk rating** (Low; medium; or high)
Risk 1: Connector/DLP misconfiguration or cross-tenant data flow leads to unintended disclosure (e.g., personal data copied to non-approved/consumer connector or another tenant) which could result in unlawful disclosure of personal data, distress, possible discrimination or identity fraud and loss of trust	Reasonable possibility	Some impact	Medium
Risk 2: Automated decision-making without adequate human review (e.g., a bot outcome triggers invoice payment)	Reasonable possibility	Some impact	Medium

Risk 3: Compromise or misuse of bot/application account credentials (caused by shared credentials or over-privileged application accounts) which could result in bulk exfiltration or tampering with data, inability to attribute actions and reputational and regulatory harm	Reasonable possibility	Some impact	Medium
Risk 4: Data-quality issues (e.g. errors caused by mis-keying) leading to automations completing in unattended mode using incorrect data	Reasonable possibility	Some impact	Medium
Risk 5: Misconfigured automation step causing leading to unintended deletion/archiving of data without backup/versioning.	Remote	Some impact	Low
Risk 6: Upstream schema/UI changes (e.g. in an application that is referenced in an unattended workflow) leads to errors or changes (e.g. wrong data field referenced or updated)	Reasonable possibility	Some impact	Medium
Risk 7: File/queue handling errors (e.g. broken connectors, lack of AI builder credits, infrastructure issues, unattended job timeouts) cause failed workflows.	Reasonable possibility	Some impact	Medium
Risk 8: Inappropriate workflows accessing systems containing medical data which could result in medical data being shared with unauthorised individuals	Remote	Some impact	Medium

17.1. Measures to mitigate (treat) risks

Against each risk you have identified, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Also indicate who has approved the measure and confirm that responsibility and timescales for completion have been integrated back into the project plan.

Risk	**Options to mitigate (treat) the risk**	**Effect on risk** (Tolerate / Terminate / Treat Transfer)	**Residual risk** (Low / Medium / High)
Risk 1: Connector/DLP misconfiguration or cross-tenant data flow leads to unintended disclosure (e.g., personal data copied to non-approved/consumer connector or another tenant) which could result in unlawful disclosure of personal data, distress, possible discrimination or identity fraud and loss of trust	• Enforce tenant- and environment-level DLP policies • Embed change control for DLP edits • Complete periodic DLP policy reviews	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases
Risk 2: Automated decision-making without adequate human review (e.g., a bot outcome triggers invoice payment)	• Developers should create “human-in-the-loop” checkpoints in unattended workflows where review / approval is required to ensure segregation of duties • Ensure flows have a full audit trail and override capability (where required)	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases
Risk 3: Compromise or misuse of bot/application account credentials (caused by shared credentials or over-privileged application accounts) which could result in bulk exfiltration or	• Store credentials in Azure Key Vault (or equivalent) • Change credentials regularly and ensure no shared credentials across application accounts	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases

tampering with data, inability to attribute actions and reputational and regulatory harm	• All accounts should have permissions based on the principle of least privilege • Completed periodic access reviews		
Risk 4: Data-quality issues (e.g. errors caused by mis-keying) leading to automations completing in unattended mode using incorrect data	• Input validation (schema, format, business rules) • Targeted sampling/review of bot outputs	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases
Risk 5: Misconfigured automation step causing leading to unintended deletion/archiving of data without backup/versioning.	• Developers should consider using flows to archive rather than permanently deleted data, to ensure restoration is possible • Organisations can also consider removing permissions for application accounts to delete data within RBAC • Ensure adequate testing is completed on all flows	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases
Risk 6: Upstream schema/UI changes (e.g. in an application that is referenced in an unattended workflow) leads to errors or changes (e.g. wrong data field referenced or updated)	• Developers should use API-first integrations where possible rather than desktop flows (avoid UI selectors) • Organisations should complete regular	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases

	release-note monitoring for applications used in unattended workflows		
Risk 7: File/queue handling errors (e.g. broken connectors, lack of AI builder credits, infrastructure issues, unattended job timeouts) cause failed workflows.	• Capacity/credit monitoring for AI Builder • Flows success monitoring through Power Automate admin centre	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases
Risk 8: Inappropriate workflows accessing systems containing medical data which could result in medical data being shared with unauthorised individuals	• Unattended RPA is not approved for Clinical use • Local organisations should strongly consider whether automated workflows accessing systems containing medical systems are required and appropriate • Enforce tenant- and environment-level DLP policies • Embed change control for DLP edits • Complete periodic DLP policy reviews • Ensure flows have a full audit trail	Decision to be made by local organisation depending on use cases and risk management processes	Dependent on mitigations implemented by local organisations and on use cases

18. Further Actions

- The completed DPIA should be submitted to the PTE Helpline Service (ighelplineservice@nhsdigital.nhs.uk) for review
- The IAO should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the processing and/or system changes)

19. Signatories

The DPIA accurately reflects the processing and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

FOR PRIVACY, TRANSPARENCY AND ETHICS AND OFFICE OF THE DPO USE ONLY

20. Summary of high residual risks

Risk no.	High residual risk summary

Summary of DPO advice:

Data Protection Officer (DPO) **Signature and Date**

ICO consultation outcome:

Office of DPO **Signature and Date**

Next Steps:

- **DPO to inform stakeholders of ICO consultation outcome**
- **IAO along with DPO and SIRO to build action plan to align the processing to ICO's decision**