Data Protection Impact Assessment (DPIA) Questionnaire for

Disclosure Scotland PVG Expansion Programme

V1.0

25 March 2025

DOCUMENT CONTROL SHEET

Key Information

Title	Disclosure Scotland PVG expansion programme
Date Published/ Issued	25 March 2025
Date Effective From	01 April 2025
Version/ Issue Number	1.0
Document Type	PDF
Document Status	Live
Author	Mathew Pay (Head of HR Strategic Delivery)
Owner	Mathew Pay (Head of HR Strategic Delivery)
Approvers	Steven Munce (Head of Workforce Planning and Resources)
Contact	mathew.pay2@nhs.scot - 0141 278 2673
File Name	DPIA_PVGExpansion.pdf

Revision History

Version	Date	Summary of Changes

Approvals

Version	Date	Name	Designation
1.0	25 March 2025	Steven Munce	Head of Workforce Planning and Resources

About the Data Protection Impact Assessment (DPIA)

The DPIA (also known as privacy impact assessment or PIA) is an assessment tool which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project that involves the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner's Office (ICO), which can include substantial fines. The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.
A DPIA is not a 'tick-box' exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done.

The ICO code of practice on conducting privacy impact assessments is a useful source of advice.

Is a DPIA required?

If the process or project that you are planning has one or more the aspects listed below then you must complete a DPIA at an early stage.

		YES/NO
1.	The work involves carrying out a ***systematic and extensive evaluation*** of people's personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing. <u>Includes:</u> Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination <u>Excludes:</u> Processing with little or no effect on people	No
2.	The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.*** <u>Includes:</u> • Racial or ethnic origin data • Political opinions data • Religious or philosophical beliefs data • Trade Union membership data • Genetic data	Yes

		YES/NO
	- Biometric data for the purpose of uniquely identifying a person - Health data - Sex life or sexual orientation data - Data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data - Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive To decide whether processing is ***large scale*** you must consider: - The number of people affected by the processing, either as a specific number or as a proportion of the relevant population - The volume of data and/or the range of different data items being processed - The duration or permanence of the processing - The geographical extent of the processing activity	
3.	The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people.	No
4.	The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset.	No
5.	The work involves processing personal data about ***vulnerable groups.*** This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data.	Yes
6.	The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of finger print and face recognition for improved physical access control; new "Internet of Things" applications.	No
7.	The work involves transferring personal data across borders ***outside the European Economic Area.***	No
8.	The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.	Yes

Step One – Consultation Phase

Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:

- Key service staff e.g. those who will be managing the process.
- Technical support, especially if a new system is involved. This may involve the relevant IT supplier.
- Information governance advisors e.g. Caldicott Guardian, Information Security Officer, Data Protection Officer.

Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS Board, or what information is collected and shared about them.

Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being 'bolted on' shortly before the change is launched.

Step Two- DPIA drafting

The responsibility for drafting a DPIA will normally sit with the service area that 'owns' the change, however, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).

Step Three- Sign-off

When a DPIA has been fully completed, it must be submitted for formal review by an appropriate IG professional/ the Data Protection Officer. They will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. The Data Protection Officer will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board's Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making.

Once reviewed, the DPIA will need to be signed off by the Information Asset Owner(s) (IAOs), normally a head of service.

1. **What are you trying to do and why?**

NHSGGC is carrying out a one-off exercise to collect staff identification details (full name, current address, and date of birth) in order to submit Protecting Vulnerable Groups (PVG) scheme applications to Disclosure Scotland. This is in response to a change in legislation that requires updated or first-time PVG membership for identified roles.

Nature of Processing:

- Collection of identity data from selected staff
- Completion and submission of PVG applications by authorised NHSGGC personnel
- Processing of PVG results and appropriate employment follow-up actions

Scope:

- Applies to a defined subset of NHSGGC staff whose roles now fall under the revised PVG legislative requirements
- Data collected: name, address, date of birth (no excessive or irrelevant data)
- Temporary processing during the one-off exercise

Context:

- Legislative change requires NHSGGC to confirm PVG status for certain roles
- Safeguarding and regulatory compliance are the key drivers
- This is time-limited and not part of ongoing business-as-usual activity

Purpose:

- To meet statutory duties under the Protection of Vulnerable Groups (Scotland) Act 2007 and subsequent amendments
- To protect patients and service users by ensuring only appropriate individuals are placed in regulated roles

Assets used:

- Primarily digital forms submitted through NHSGGC secure systems
- Paper forms used only where required for accessibility
- Disclosure Scotland’s online PVG system
- Internal HR platforms and secure communication channels

Data flows:

1. Staff complete a digital or paper form and submit to NHSGGC
2. Authorised staff enter the data into Disclosure Scotland’s PVG system
3. PVG results are returned to NHSGGC and stored securely
4. HR reviews the results and takes any necessary action

Necessity and proportionality:

- The data collected is the minimum required to complete a PVG application
- Processing is time-limited, tightly controlled, and for a lawful purpose
- All data is handled securely, with access limited to authorised personnel
- Results are used solely for safeguarding and role suitability assessment

2. **Data Protection by Design & Default – Give details of how the processing or system will benefit the Data Subject and ensure the Board will comply with the UKGDPR Data Processing Principles as listed in S.16.**

This one-off PVG processing exercise has been designed to ensure NHSGGC complies fully with the UK GDPR principles while delivering a clear safeguarding benefit for staff, patients, and the public.

Benefits to the data subject:

- Confirms staff members' eligibility to work in regulated roles, supporting their continued employment or deployment.
- Enhances workplace safety by ensuring all individuals in regulated positions have undergone appropriate vetting.
- Promotes trust and confidence in NHSGGC as a responsible and compliant employer.

Principle	How it is met
Lawfulness, fairness, transparency	Processing is based on legal obligation and substantial public interest. Staff are informed of the purpose, use, and legal basis for PVG checks.
Purpose limitation	Data is collected solely to support Disclosure Scotland PVG applications and is not reused for unrelated purposes.
Data minimisation	Only the minimum necessary data (name, address, date of birth) is collected to complete the application.
Accuracy	Data is provided directly by the data subject, reducing risk of errors. Staff are given the opportunity to verify details before submission.
Storage limitation	Data is retained only as long as needed to complete the PVG process and record outcomes. Retention is in line with NHSGGC HR and PVG handling policies.
Integrity & confidentiality	All data is stored securely within NHSGGC systems. Paper forms are used only where required and handled with strict access and disposal controls.
Accountability	A DPIA is being completed, and named responsible staff are managing and auditing the process to ensure compliance.

Data Protection by design:

- Digital forms are used by default to reduce handling risk.
- Role-based access controls ensure only authorised staff can process PVG-related data.
- Paper forms are made available only to accommodate accessibility needs and are handled securely.
- No unnecessary duplication or centralisation of data beyond what is operationally required.

Data Protection by default:

- Only essential fields are included in forms.
- Results from Disclosure Scotland are shared only on a need-to-know basis.
- Internal systems are configured to limit storage and access in line with data minimisation.

3. **What personal data will be used?**

Categories of individuals	Categories of personal data	Any special categories of personal data	Sources of personal data
NHSGGC staff in regulated roles (as defined by PVG legislation)	• Full name • Current address • Date of birth	None directly collected. However, the PVG process will result in Disclosure Scotland processing and returning information relating to criminal convictions (Article 10 data)	Provided directly by the data subject via digital or paper form

4. **What legal condition for using the personal data is being relied upon?**

Legal condition(s) for *personal data*	Legal conditions for any *special categories of personal data*
UK GDPR Article 6(1)(c) - Legal obligation and/or Article 6(1)(e) - Public task (depending on employment basis and contractual terms)	UK GDPR Article 10 - Processing of criminal conviction and offence data is authorised by law Supported by the Protection of Vulnerable Groups (Scotland) Act 2007, which mandates suitability checks for regulated work

5. **Describe how the personal data will be collected, used, transferred and if necessary kept up to date.**

Collection:

- Staff identified as requiring PVG checks will be contacted directly.
- Personal data (full name, current address, date of birth) will be collected using secure digital forms by default.
- Paper forms will be available where required for accessibility.

Use:

- The collected data will be used solely to complete PVG scheme applications via Disclosure Scotland.
- NHSGGC staff responsible for PVG submissions will input the data into the online PVG system.
- No profiling, automated decision-making or unrelated processing will occur.

Transfer:

- Data is submitted to Disclosure Scotland via their secure online platform.
- Paper forms, where used, are held securely and data is transcribed into the system before being securely destroyed or filed according to NHSGGC document retention policies.
- PVG results are returned to NHSGGC through Disclosure Scotland’s secure reporting mechanisms and accessed only by authorised HR staff.

Updating data:

- Staff are responsible for checking and confirming the accuracy of their personal data before submission.
- Any errors identified are corrected before submission to Disclosure Scotland.
- PVG scheme records are not routinely updated post-submission unless a material change triggers a new application.

6. What information is being provided to the people to whom the data relate to ensure that they are aware of this use of their personal data? – This is the 'right to be informed' and information such as privacy notices may be included as an attachment.

Staff are informed about the purpose and use of their personal data through:

- A targeted staff communication (email or letter) explaining the need for the PVG check, what data is being collected, how it will be used, and their rights under UK GDPR.
- Access to the NHSGGC Employee Privacy Notice, which outlines how personal data is processed in line with GDPR requirements.
- A dedicated PVG-specific privacy statement or data collection notice accompanying the digital or paper form, explaining:
  - What data is required and why
  - The legal basis for processing
  - Who will have access to the data
  - How long the data will be retained
  - Contact details for queries or concerns, including the Data Protection Officer

This information is published on HR Connect.

This ensures the organisation meets the UK GDPR right to be informed and that staff are fully aware of the data processing activity before providing their information.

7. How will people's individual rights in relation to the use of their personal data be addressed by this process?

The following UK GDPR rights are recognised and upheld in the PVG checking process:

Right to be informed	Staff receive clear information via privacy notices, covering what data is collected, why, and how it is used.
Right of access	Staff can request access to their personal data held by NHSGGC, including any data submitted as part of the PVG process.
Right to rectification	Staff can correct any inaccurate personal data before submission. Errors identified post-submission are managed case-by-case.
Right to erasure	Not applicable where data is processed under a legal obligation or public task.
Right to restrict processing	Staff may request restriction of their data in limited circumstances, but this may be overridden due to legal obligations.

Right to object	Staff can raise objections, but NHSGGC may continue processing where legally required to fulfil safeguarding duties.
Rights related to automated decision-making	Not applicable. The process involves no automated decisions or profiling.

8. For how long will the personal data be kept?

Personal data collected for the purpose of this one-off PVG check will be retained in line with the NHSGGC Records Management and Retention Policy and relevant NHS Scotland retention schedules.

- Data collected from staff (e.g. identity details submitted for the PVG application) will be retained only for as long as necessary to complete the PVG application process and confirm outcome receipt.
- Outcome records (i.e. confirmation of PVG status and clearance date) will be retained as part of the employee's HR file in line with the retention period for recruitment and safeguarding checks, which is typically six years after employment ends.
- Paper forms, where used, will be securely destroyed once transcribed and no longer needed.

All retention and disposal actions will be carried out securely and in line with NHSGGC data protection procedures.

9. Who will have access to the personal data?

Access to personal data collected for the PVG process will be strictly limited to:

- Authorised NHSGGC HR staff responsible for managing the PVG application process.
- Line managers or appointing managers, but only where necessary to confirm an individual's clearance status for deployment.
- Disclosure Scotland, as the external authority processing PVG applications and issuing results.
- Information Governance or Data Protection Officer, if required for audit, support, or to handle any data rights requests or incidents.

Access is granted on a role-based, need-to-know basis and governed by NHSGGC's information governance, confidentiality, and access control policies. All users accessing this data are trained in GDPR compliance and confidentiality obligations.

10. Will the personal data be routinely shared with any other service or organisation? – If yes, provide details of data sharing agreement(s) and any other relevant controls. Advice on data sharing requirements is in the Scottish Information Sharing Toolkit.

Yes - but only with Disclosure Scotland, for the purpose of processing PVG scheme applications.

Details:

- Personal data (full name, address, date of birth) is shared with Disclosure Scotland to enable legal vetting under the Protection of Vulnerable Groups (Scotland) Act 2007.
- This is a routine and lawful data sharing activity, necessary for safeguarding and compliance with regulated role requirements.

Controls in place:

- The data is submitted via Disclosure Scotland's secure online platform, using official channels approved by the Scottish Government.
- NHSGGC staff involved in this process are trained in handling personal data and operate within secure systems and policies.
- Data sharing is covered by the statutory relationship between NHSGGC and Disclosure Scotland, and subject to oversight from NHSGGC's Information Governance function.

There is no routine sharing of this data with any other external organisations or third parties.

11. Will the personal data be processed by a Data Processor e.g. an IT services provider?

No, not in the context of this PVG checking exercise.

Personal data is:

- Collected and processed directly by NHSGGC staff.
- Submitted to Disclosure Scotland, which acts as a separate data controller - not a processor on behalf of NHSGGC.
- Handled through internal NHSGGC systems or secure official platforms provided by Disclosure Scotland.

If any internal IT systems or support services are involved, they operate under NHSGGC's direct control and are not acting as independent data processors for this specific processing activity.

12. Describe what *organisational* controls will be in place to support the process and protect the personal data.

Type of Control – examples	Description
Information security and related policy(ies)	NHSGGC policies on Information Governance, Data Protection, and Secure Handling of Personal Data are in place and apply to all staff involved.
Staff training	All relevant HR and administrative staff have completed mandatory GDPR and Information Governance training, with updates for PVG handling as needed.
Adverse event reporting and management	Any suspected data breach or inappropriate access is reported and managed in line with NHSGGC's Incident Reporting Policy and IG response protocols.
Physical access and authorisation controls	Paper forms (if used) are stored in secure, access-controlled areas. Digital systems are protected by login credentials and role-based access.
Environmental controls	Offices handling physical data are secure, with restricted access, CCTV coverage where applicable, and lockable storage facilities.

Type of Control – examples	Description
Information asset management including management of backups and asset disposal	Digital data is stored within NHSGGC's approved systems with appropriate backup and disposal routines. Paper forms are securely destroyed when no longer required using the on-site shredding facilities.
Business continuity	Business continuity plans are in place for digital systems. The short-term nature of the PVG exercise limits operational risk exposure.
Add others where applicable	**Audit and compliance checks** Spot checks or audits may be carried out by Information Governance or HR management to ensure compliance with policy and process.

13. Describe what *technical* controls will be in place to support the process and protect the personal data.

Type of Control – examples	Description
System access levels and user authentication controls	NHSGGC systems used in the PVG process are protected by secure login credentials. Access is restricted to authorised HR staff on a need-to-know basis.
System auditing functionality and procedures	User activity on relevant systems is logged and auditable. Any access to personal data is traceable and monitored for compliance.
Operating system controls such as vulnerability scanning and anti-virus software	All NHSGGC devices are managed centrally, with regular patching, anti-virus protection, and vulnerability scanning in line with NHS national standards.
Network security such as firewalls and penetration testing	NHSGGC networks are protected by firewalls, intrusion detection systems, and regular penetration testing.
Encryption of special category personal data	While special category data is not directly collected by NHSGGC in this process, any sensitive data (e.g. PVG outcomes) is transmitted and stored securely, with encryption in place where required.
Cyber Essentials compliance(if applicable)	NHSGGC meets the standards outlined in Cyber Essentials and adheres to NHS Scotland cybersecurity frameworks.
System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)	Standard Operating Procedures and Information Security Policies are in place for HR and IG teams managing the PVG process.
Details of ISO27001/02 accreditation (if applicable)	NHSGGC aligns with ISO 27001/27002 principles for information security management, though formal accreditation may apply at the national NHS level.

Type of Control – examples	Description
Add others where applicable	Data entered into Disclosure Scotland's platform is protected via secure HTTPS protocols. Internal file transfers follow NHSGGC secure transfer procedures.

14. Will personal data be transferred to outside the European Economic Area (EEA) or countries without a European Commission-designated adequate level of protection?

No - all personal data collected and processed as part of this PVG exercise will be:

- Stored and handled within NHSGGC systems, based in the UK.
- Submitted to Disclosure Scotland, a Scottish Government agency operating entirely within the UK.

No part of the data processing involves international transfers, and no data will be sent outside the UK or EEA.

15. Describe who has been consulted in relation to this process – e.g. subject matter experts, service providers, service users.

The following individuals and groups have been consulted to ensure the PVG checking process is compliant, proportionate, and operationally sound:

- HR and Workforce Planning leads - to identify affected roles and coordinate the data collection and application process.
- Information Governance (IG) team - to review data protection risks, legal basis, and handling procedures.
- Data Protection Officer (DPO) - to review the DPIA and provide assurance on UK GDPR compliance.
- Staff-side representatives and Partnership Forum - to support transparency with affected staff and ensure awareness.
- Line managers - to identify staff in scope and provide appropriate operational support.

16. In light of what is proposed, indicate what level of risk has been identified in relation to the following data protection principles:

Principle	***Low/ Green***	***Medium/ Amber***	***High/ Red***
Personal data is processed in a fair, lawful and transparent manner	✓		
Personal data is collected for specific, explicit and legitimate purposes	✓		
Personal data is adequate, relevant and limited to what is necessary	✓		
Personal data is accurate, and kept up to date	✓		

Principle	***Low/ Green***	***Medium/ Amber***	***High/ Red***
Personal data is kept no longer than necessary	✓		
Personal data is processed in a manner that ensures adequate security	✓		

17. Risks and actions identified. List all that you have identified and ensure that these integrate properly with our NHS Board's risk management process:

Description	Likelihood	Consequence	Overall Risk rating (LxC)	Mitigation/ Actions	Residual Risk	Risk Owner	Date
Unauthorised access to personal data during collection or processing	Low	Moderate	Low (e.g. 2 x 3 = 6)	Role-based access controls, staff training, secure storage for paper forms, data minimisation	Low	Head of Workforce Planning and Resources	April 2025
Inaccurate or outdated personal data used in PVG application	Low	Minor	Low (e.g. 2 x 2 = 4)	Data is self-submitted by staff with opportunity to verify before submission	Low	Head of Workforce Planning and Resources	April 2025
Loss or misplacement of physical forms used for accessibility	Low	Moderate	Low (e.g. 2 x 3 = 6)	Limit paper use, store securely, digitise promptly, and dispose of securely in line with retention policy	Low	Head of Workforce Planning and Resources	April 2025
Failure to comply with GDPR data retention principles	Low	Moderate	Low (e.g. 2 x 3 = 6)	Apply NHSGGC Records Management policy and track retention periods	Low	Head of Workforce Planning and Resources	April 2025
Staff not fully informed about data use or rights	Low	Moderate	Low (e.g. 2 x 3 = 6)	Use clear privacy notices and staff communications prior to data collection	Low	Head of Workforce Planning and Resources	April 2025