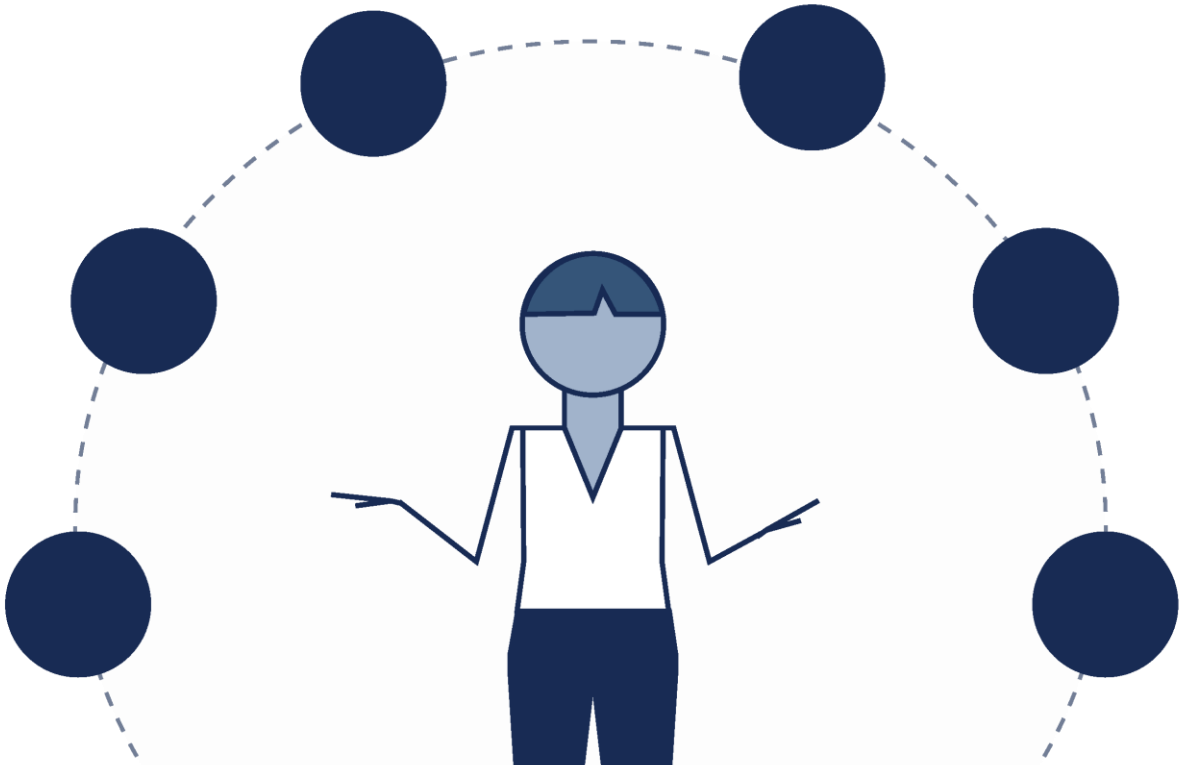
DPIA for VMS

Data Protection Impact Assessment (DPIA) for Northern Ireland's Vaccine Management System (VMS)

Last published: November 2026



Project Name / *DPIA Reference*	
Vaccine Management System (VMS) / *VMS 2022* (updated November 2026 to include the adult pneumococcal programme)	
Data Controller	**Data Protection Officer (DPO)**
PHA NI (Public Health Agency Northern Ireland)	Helen O'Hare
Contributors	
VMS Team (PHA)	

Version	Published
v3.2	February 25, 2021
v4.0	February 7, 2023
v5.0	March 31, 2023
v6.1	October 19, 2023
v6.7	May 20, 2024
v6.8	September 17, 2024
v6.9	April 29, 2025
v7.0	July 21, 2026
v7.1	November 5, 2026

1. Table of Contents

Section	Description
1. Table of Contents	Describes and links to sections in this document.
2. What is this DPIA for?	Describes what this document is and the consultation process.
3. VMS Context and Background	Describes the VMS: project aims, ownership and main components.
4. Data Processing Overview	Describes the purpose, necessity, scope, nature, and context of processing data within the VMS.
5. VMS Risks Relating to Data	Describes the VMS risks relating to data, and what measures are being put in place to minimise those risks.
6. DPIA Sign-off	A formal sign-off of this document and commentary from the DPOs.
7. Appendix	Includes extra information referenced throughout this document.

2. What is this DPIA for?

A Data Protection Impact Assessment (DPIA) is an essential part of VMS' accountability and legal obligations as a project which processes the personal data of citizens in Northern Ireland.

This document aims to articulate the why, what, who, how of VMS data processing, and covers many areas. It has been updated in November 2026 to include the pneumococcal programme.

The DPIA is a tool used by project leads to assess, understand and set out appropriate mitigations for any data protection and privacy risks associated with VMS processing. These assessments have helped and continue to ensure privacy by design within VMS.

2.1 DPIA Consultation

Formal public consultations are usually required for a project of this magnitude. However, due to the urgent requirement to establish and operationalise the VMS during the COVID-19 pandemic, a formal consultation was not undertaken before VMS was built. Since then, regular engagement has been undertaken with a wide range of stakeholders as listed in Appendix A and conversations have covered all topics a consultation would typically cover.

The VMS team remain in close contact with our counterparts in England and the other devolved administrations as well as the Republic of Ireland to share learning.

The VMS team has liaised extensively with the PHA Personal Data Guardian (PDG) and lead clinicians, PHA DPO, DoH DPO, Trust IG/DPO leads, and Directorate of Legal Services, taking account of advice and comments and ensuring that appropriate measures are in place to safeguard individual's personal data. There has also been significant engagement with the ICO office in NI, which is ongoing.

3. VMS Context and Background

3.1 Purpose of VMS

A vaccination programme for both COVID and seasonal flu was commissioned in Northern Ireland (NI). The primary technology solution used to support this programme is known as the Vaccine Management System (VMS or "the VMS"). VMS has since expanded to include other vaccination programmes.

VMS is formed of several components working together as one single solution, enabling:

- …citizens to book appointments
- …administrators to schedule and manage vaccination clinics
- …healthcare professionals to record vaccines

- …GPs to know which patients under their care have been vaccinated
- …data scientists to analyse vaccination data in the interests of public health protection
- …and many more capabilities

The VMS is intended for use in any vaccination settings where a vaccination is delivered, including: GP practice, Trust-led vaccination clinic, care or residential home, patient's home (housebound), ward (long stay patients) mobile clinics and participating community pharmacies.

3.2 Ownership of VMS

The building of VMS started in December 2020 and the joint data controllers for the system (under UK Data Protection legislation) were the Health and Social Care Board (HSCB) and PHA.

From April 2022 full operational responsibility for the maintenance of the VMS transferred wholly to Public Health Agency (PHA), in continued partnership with a wide range of delivery partners, including: APTVision, Kainos, Business Services Organisation (BSO) and the Belfast Trust.

As the HSCB closed and the functions transferred to the newly formed Strategic Planning and Performance Group (SPPG) within DoH on 1 April 2022, the Department took on the joint controller function, previously owned by HSCB, along with the PHA for the Vaccination Management System (VMS).

From 1 April 2023, Public Health Agency (PHA) took on single control ownership of the Vaccine Management System (VMS).

3.3 Product overview of VMS

Different user groups interact with different VMS technologies, as briefly described in the table below. It should be noted that whilst this list is correct at the time of writing, the VMS continues to evolve and this DPIA will continue to be reviewed and updated as required.

	Product	Description of use
Citizen	**Booking Platform**	○ Book an appointment to receive a vaccination ○ Manage and view appointments booked using this platform ○ Send notifications to invite citizens to book and reminders to attend appointments, such as through vaccine 'recall'
Healthcare workers	**Booking Platform Admin**	○ Setup locations and available time slots for appointments

		○ Reschedule and cancel booked appointments
Healthcare workers	**VMS**	○ Record vaccinations ○ View patient vaccination records
Other*	**NIHAP**	○ Vaccination records are used for analytics within HSCNI
Other	**Data Quality**	○ Identify and fix data quality issues with vaccination records, such as incomplete, wrong, or missing records
Other*	**HSCNI Honest Broker Service**	○ To provide safe access to vaccination data from VMS for research

** Those marked are outside of VMS remit and are seen as data processors for the purposes of this document.*

4. Data Processing Overview

What is "data processing"?

Processing data means any of the following: create, store, use, share, archive or destroy. In one form or another, VMS does all these things.

For the purposes of this DPIA, we describe only *personal data* processing. Personal data relates to a living individual who can be identified either directly from the data or from the data in combination with other data that may come into VMS.

Who does VMS process personal data on?

VMS processes data on two groups of users: citizens and healthcare workers (including clinical and nonclinical staff).

As a national vaccination programme, the VMS contains personal data relating to most of the vaccine-eligible population of Northern Ireland, as well as all Trust vaccination staff, GPs and participating pharmacies.

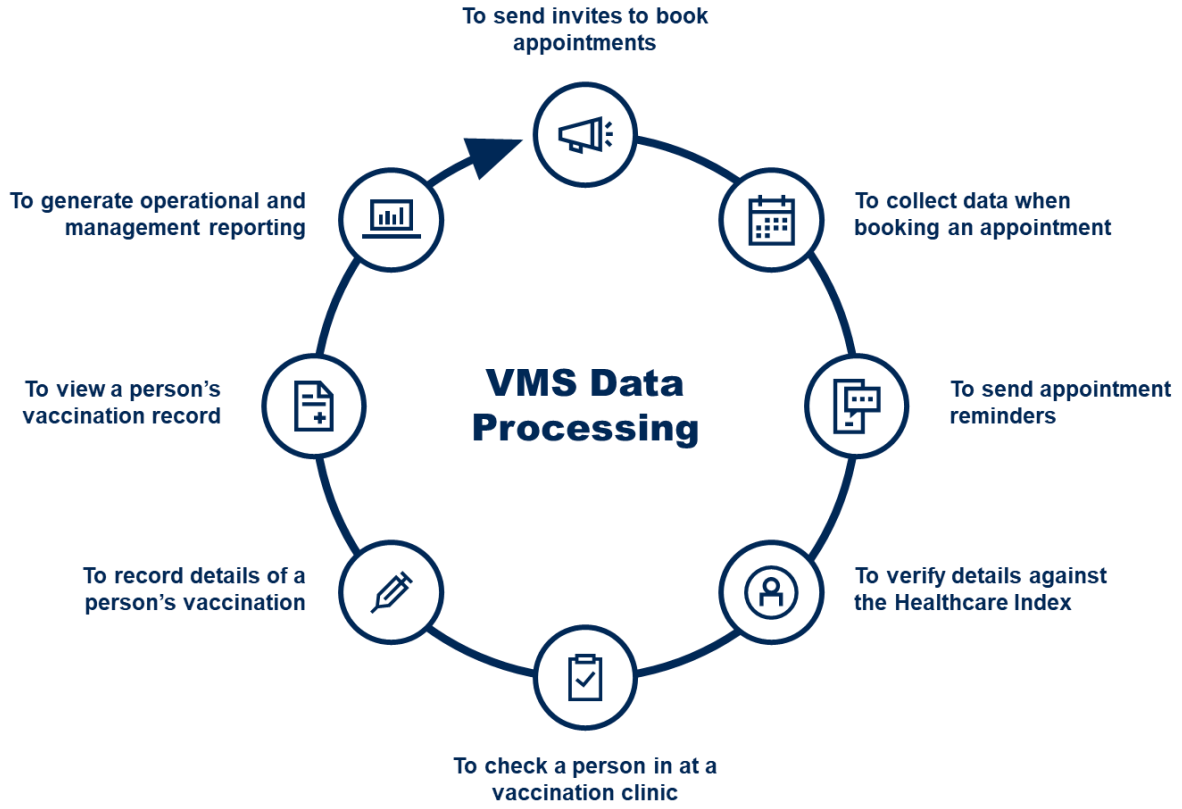
The VMS therefore contains personal data on both children and vulnerable individuals – particularly data relating to clinical vulnerability.

The VMS is not novel in the sense that vaccinations have been recorded digitally for many years, however the processing usage of personal data (see below) is considered novel.

Why does VMS process personal data?

The primary purpose of the processing of personal data in VMS is to ensure the safe Covid-19, flu, shingles, MMR, pertussis, RSV, MenB and pneumococcal vaccinations of citizens in Northern Ireland.

The VMS may process an individual's personal information for the purposes shown in the diagram below:



Additionally, the VMS may send or receive personal information to external systems for the following purposes (see point 4 in particular for the purposes of data transfer from CHS to VMS).

1. To/from the citizen's GP Surgery, to enable their GP to maintain a complete medical record
2. To/from the PHA data lake (NIHAP), to conduct data quality review and fixes, and support health surveillance and health research (for example, establishing geographic areas of low vaccine uptake)
3. To/from other nations (including the UK), to send a person's vaccination records back to the country from which they are a citizen (ceased operation in 2024)
4. From the NI Child Health System (CHS) to maintain a complete medical record for children's flu vaccinations

What personal data does VMS process?

Whenever possible VMS collects the minimal amount of personal data required to fulfil the purposes listed above. VMS processes personal data at every point of interaction with the system, for example collecting or modifying data.

The primary source of VMS personal data is either:

- directly from citizens (when booking or checking into a vaccination clinic); or
- from the Health and Care Number (HCN) Index, which contains the "master" of personal data for all citizens registered with GPs; or
- from the Child Health System, when childhood flu vaccination records are transferred electronically to VMS

There are also extreme occasions when personal data must be collected manually (for example, when computer networks are offline), therefore staff may resort to paper or approved Excel spreadsheets for collection of personal data to be entered onto the VMS once available.

The below list includes all data fields currently being processed by VMS:

- *Health Vaccination*
    - Vaccine site
    - Date of Vaccination
    - Reason patient not suitable for vaccine
    - Reason patient is eligible for vaccine
    - Product Name
    - Vaccine – dose given
    - Vaccine – Batch Number
    - Informed Consent
    - Vaccination Centre
    - Name of Vaccinator
- *Personal Identification*
    - Age
    - Date of Birth
    - Surname
    - Sex
    - Ethnicity
    - First Name
    - Family Name
- *Health/Medical Data*
    - Health & Care Number
- *Contact Information*
    - Home Address
    - Phone Numbers
    - Email

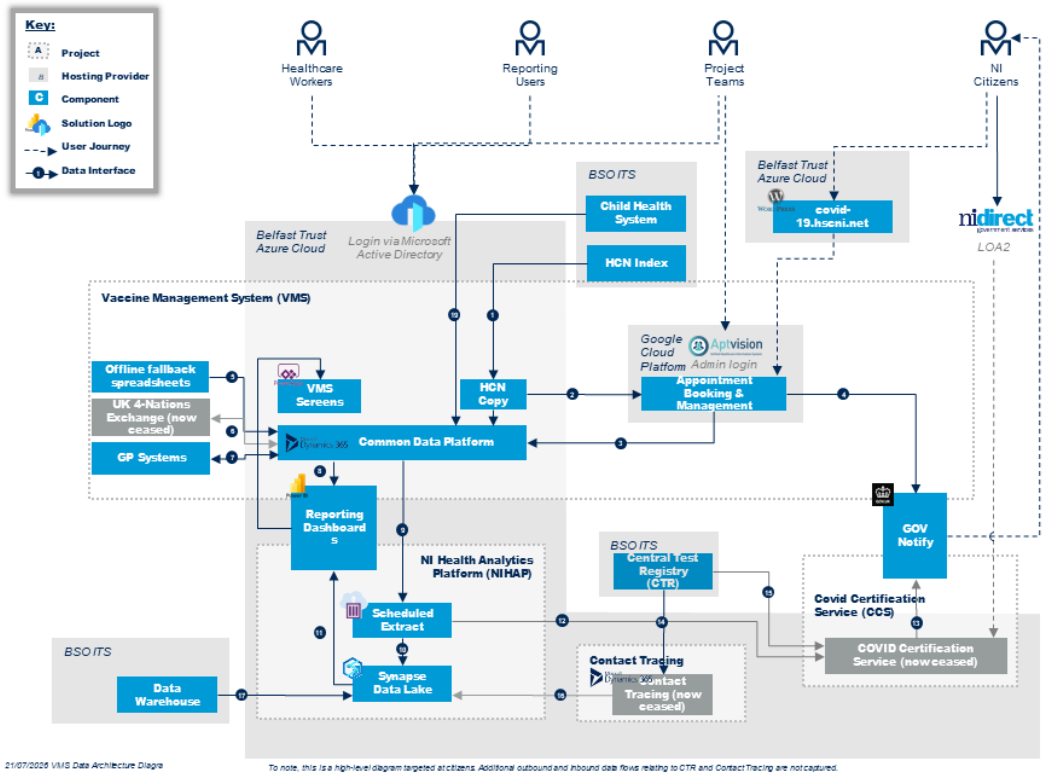
    - RQIA Code (care home staff and residents)
    - DENI Number (school attended)
    - Pregnancy
    - Medical considerations (e.g. allergies, previous reaction to vaccine)
- *HSC Staff (in addition to above)*
    - Place of Work
    - Job role
    - Staff Number

To note, all SMS and email appointment confirmation and reminder messages come from **HSC vaccine** to the mobile or email address supplied at booking. If citizens use the online system they will receive confirmation of their appointment bookings and reminders of appointments either by email or text SMS.

The messaging mechanism may also be used for the purposes of Vaccine 'Recall', which involves sending reminders, via text SMS or email, to citizens who had previously had a vaccine to advise that they may be eligible for another vaccine.

How does VMS process personal data?

Please refer to the Data Architecture Diagram below, developed in collaboration with PHA, which outlines relevant outbound and inbound data flows. To note, there are several external data processors. COVID Certification Service (CCS), COVID-19 contact tracing and UK 4-Nations data sharing have now ceased, and data interfaces coloured grey, it will be removed from future versions of the diagram.



Who does VMS share personal data with?

There are several organisations which process data for the VMS – these are known as a *data processors*. VMS' data processors are appointed under Data Processors Agreements in compliance with Article 28 of the UK GDPR.

Contracts, Data Sharing Agreements (DSAs) and Memorandum of Understanding (MoUs) are in place to govern relationships with the below data processors and sub-processors which set out the obligations of each party and the data controller's obligations and rights regarding the data that is being processed. All contracts adhere to established BSO Procurement and Logistics Services (PaLs) processes with legal input provided by BSO Department of Legal Services (DLS).

Under Article 28(1) and the established arrangements for the overall operational responsibility for VMS, the PHA is responsible for ensuring that data processors listed below can provide "sufficient guarantees" (in terms of its expert knowledge, resources, and reliability) to put in place appropriate measures to ensure any data processing complies with the UK GDPR and protects the rights of individuals.

The following provides a list of data processors involved in delivery of the system:

- **Kainos** is a system integrator providing VMS platform for storage and processing of vaccination records

- **APTVision** are medical systems software development company chosen to develop the VMS booking and scheduling platform and are responsible for the configuration of the booking system and interim VMS database. They are regarded as a processor contracted by PHA. APTVision will provide support on an ongoing basis to the VMS booking system for the duration of its operation, as part of their contract. Their services are delivered via UK GDPR compliant G-Cloud contracts.

- **Business Services Organisation** (BSO) is a statutory organisation providing services as a data processor for PHA. BSO are responsible for first-line support for VMS, as well as monitoring and managing all Microsoft contracts as commissioned and monitored by PHA. They are responsible for all VMS environments, user access and provision of new user hardware (PC and phones). BSO ITS are responsible for the supply and maintenance of user hardware. PHA have overarching SLAs with the BSO for services including ITS. Their services are managed via appropriate agreements with PHA.

- **Belfast Health and Social Care Trust** (BHSCT) is a statutory organisation providing VMS cloud hosting services. Their services are managed via appropriate agreements with PHA.

- **Microsoft** are responsible for, within the Microsoft Azure environment including the Dynamic 365 environment, software upgrades, security patching and updates for the Vaccine Management System; these are published via MS Office 365 portal that BSO ITS have access to.

- **GOV Notify (Cabinet Office)** enables the VMS to send emails and text messages to citizens, including invitations to book online, vaccine 'recall', booking confirmations and appointment reminders.

- **Google Analytics** is used to measure use of the booking platform by citizens, no personal data is shared with Google Analytics. Google Analytics uses cookies to remember a user's behaviour. Data entered into the booking platform as part of the booking process is not shared with Google Analytics, and the data collected by Google Analytics is never combined with personal data collected by VMS.

As well as the processing carried out by VMS data processors above, VMS previously enabled secure cross sharing of COVID-19 vaccination records between Northern Ireland and separate health care data controllers in England. Cross sharing ceased following the closure of the COVID Certification Service in January 2024, earlier versions of this document provide further details.

Requests for VMS data from researchers are managed by the HSCNI Honest Broker Service. The Honest Broker Service is the Trusted Research Environment (Also sometimes referred to

as a Secure Data Environment or Data Safe Haven) for Health and Social Care Northern Ireland.

The Honest Broker Service provides a highly secure processing environment where accredited researchers can access de-identified data, along with the tools required to analyse it.

The service also provides access to anonymised, pseudonymised or aggregate data to internal Department of Health and Health and Social Care Northern Ireland organisations (for example for the purposes of clinical audit, service improvement and health protection).

It is commissioned by the Department of Health and the Northern Ireland Trusted Research Environment (NITRE) Strategic Board and has appropriate governance and approvals processes, including sign off and input from all HSC data controller organisations, which own the data processed by HBS for these purposes.

The Honest Broker Service operates under the 5 Safes Framework which is a commonly adopted approach across equivalent bodies in the UK. This provides an end to end privacy by design process intended to provide a number of controls which greatly reduce the likelihood of sensitive data being leaked or misused during research.

Safe Projects - All projects are scrutinised by HSC Data Access Committee. Projects must be in the public interest, consider ethical considerations and be of relevance to Health and Social Care Policy.

Requests to link or match VMS data will, in the first instance, be directed to the BSO Honest Broker Service (HBS) who will engage with the researcher(s) and the DHCNI Data Analytics Team. The PHA Information Asset Owner for VMS is represented on the Data Access Committee. Only anonymised data will be provided for approved research.

Safe People – The researchers who access the data are trained in data security and personal responsibility and are subject to robust legal contracts. Researchers accessing data via the Honest Broker Service must be accredited researchers (having completed the ONS Safe Researcher Training or equivalent).

Safe Setting – The Honest Broker Service operates on a “Data Access” rather than “Data Dissemination” principle. Researchers are provided with a highly secure computing environment through which they access the data provisioned along with the tools needed to carry out analysis. Information cannot be copied directly onto the research institution network but is accessed through the controlled environment (overseen by the HBS). This provides additional security during the analysis stage.

The Safe Setting used by the Honest Broker Service is the Honest Broker Service tenancy of the Secure e-Research Platform (SeRP), managed in collaboration with Swansea University.

Safe Data – Researchers are only allowed access to data which has been de-identified to ensure that they cannot learn sensitive personal information about data subjects during the analysis.

The Honest Broker Service and VMS team will collaborate during the linkage process to create extracts that can be linked using privacy preserving techniques – Health and Care Numbers will be hashed during the linkage process using an agreed hashing algorithm and a shared project specific secret Salt will be applied[1].

This protects privacy while the Honest Broker Service staff are preparing data from multiple sources (For example VMS data and secondary care hospital admission data).

The hashed and salted health and care numbers will be replaced with a unique Study_ID for each data subject by the Honest Broker Service prior to providing researchers access to data in the Safe Setting.

Safe Outputs - Researchers can access the detailed de-identified information through the Secure Data Environment, but the only outputs they can request be removed from the environment are the fully anonymised, aggregated data that they require for writing up their research findings.

All outputs will have been checked by the Honest Broker Service prior to release to ensure that individuals cannot be re-identified.

The aim is to enable non-identifiable clinical data to be safely shared to maximise the uses and health service benefits which can be gained from it, including Planning, Commissioning of services and Public health monitoring and to ensure the confidentiality of patient identifiable information is maintained at all times.

Where do we store personal data?

VMS data processing mostly takes place within the UK area and as such is subject to UK Data Protection legislation, including UK GDPR and the Data Protection Act 2018.

[1] A secure hashing algorithm is a one-way process that converts a string of "plain text" into a new long string of characters, known as a digest.

The same input will always produce the same hashed Digest so if for example the Health and Care Numbers were hashed on two different datasets it is possible to carry out record linkage, as long as the same hashing algorithm has been used. A "Salt" is a string of characters that is appended to the input data. Applying a new secret salt for each linkage project ensures that data cannot be cross referenced between different projects.

Data processing also takes place outside the UK area – specifically for product delivery and service & support. This processing takes place in line with Chapter V, Article 45 UK GDPR on the basis of an adequacy decision and in line with the guidance from the Information Commissioner's Office[2].

VMS data is stored in three places, as described below:

- **Belfast Trust Microsoft Azure Tenancy** – all Microsoft applications within VMS (primarily core VMS vaccine recording) are hosted by Belfast Trust's Microsoft Azure tenancy.
- **Google Cloud Platform** – the Aptvision application (used primarily for citizens to book appointments) is hosted within the UK Google Cloud Platform.
- (Uncommonly) via email – which is used for encrypted sharing of information required to facilitate support for VMS, for example between BSO and PHA to enable the investigation of specific vaccination records on request from VMS users.

How long do we process personal data for?

We will only retain your data for as long as necessary, in line with our Retention and Disposal Schedule and specific guidance issued by the Department of Health in Northern Ireland (Good Management, Good Records) which can be found here.

What rights do data subjects have?

The UK GDPR sets out the 8 rights that individuals have in respect of their data. These have been considered in respect of the VMS as follows:

1. **The right to be informed**

   Individuals are provided with information in the VMS Privacy Notice about the collection and use of their personal data for the VMS, including what personal data is collected, the purposes for collecting, retention periods and potential sharing of data. They are also provided with information about their data subject rights.

   The Privacy Notice can be found here.

   In addition, the PHA, NI Direct and GOV.UK websites also include a wide range of information about the vaccine programmes to ensure citizens are informed.

2. **Right of access**

   Individuals can ask for copies of the information that we hold about them. HSC has an established subject access request (SAR) process to ensure that requests are dealt

[2] Read more about Adequacy Regulations at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

with promptly and appropriately and individuals are advised in the Privacy Notice about how they can make a SAR.

3. **Right to rectification**

   Individuals can ask to have inaccurate personal data corrected or completed if it is incomplete. Those administering vaccines will verify data at vaccination appointments. Individuals are also advised in the privacy notice of how they can request rectification of their information.

4. **Right to erasure**

   GDPR introduced a right for individuals to have personal data erased ('the right to be forgotten'), however the right is not absolute and only applies in certain circumstances.

5. **Right to restrict processing**

   Individuals have the right to request the restriction or suppression of their personal data, however the right is not absolute. While individuals can request that the vaccine programme stops processing their data, as set out in number 4 above, the data held will still need to be processed for the purpose of public health protection and personal clinical record keeping.

6. **Right to data portability**

   Individuals can ask the vaccine programme to share their information with another organisation (although this may not always be possible).

7. **Right to object**

   Individuals have the right to object to the processing of their personal data, including when the lawful basis for processing is public task. However, this is not an absolute right, and processing can continue if there are compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual.

8. **Rights relating to automated decision-making**

   Automated decision-making relating to personal data, without any human involvement, may be performed during data quality improvement exercises. However, it should be noted this is only done when clinical experts have agreed that the automated process can replicate a human with very minimal levels of risk.

Individuals wishing to exercise one of these rights are advised within the Privacy Notice to contact the DPO, Helen O'Hare.

Email: DPO.PHA@hscni.net

To what extent is VMS data processing necessary and proportionate?

In Northern Ireland, the COVID-19 and seasonal Flu vaccination programme, along with RSV, pertussis, Shingles, adult MMR, adult MenB and adult pneumococcal is supported by the VMS to allow citizens to receive their vaccinations and to provide a central regionalised record of all vaccinations.

Only the minimum data set is processed, to enable safe vaccination and to provide demographic data to identify and manage uptake for public health surveillance.

The personal data collected through the VMS will only be used for purposes of vaccination, public health surveillance and research.

Vaccination is an established and recognised methodology for controlling and reducing the spread of communicable infectious diseases, that is used nationally and internationally.

Developing NI's VMS was necessary to delivering the COVID-19 vaccine rapidly to the population because the current mixed IT/paper-based vaccine delivery mechanism in place was not geared to delivering vaccines at volume in a pandemic scenario. A specifically designed VMS ensured equity of access to the vaccine across population cohorts through a single, consistent scheduled booking system.

The VMS is proportionate given the preexisting vaccine delivery mechanism's inability to support a pandemic scenario. It does this by:

- Ensuring the DOH meets its obligations regarding the protection of patient data and confidentiality
- Ensuring the DOH use best practice in the care and safety of any person receiving the vaccine
- Reducing or eliminating the clinical and information governance risks associated with the existing vaccination systems and processes.
- Providing a fit for purpose platform that can be used again in future pandemic outbreaks and for consistent vaccinations generally. Improving the accuracy of NI clinical/vaccine data recording and reporting
- Capturing data relating to adverse drug reactions post administration of the vaccine and within the observation period
- Making vaccine data readily and securely accessible to those authorised to process it
- Helping support standardised clinical and GP workflow management in all vaccination settings.

The Lawful Basis for Processing

The lawful basis for processing personal information according to the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 is:

- UK GDPR Article 6(1) (e) – the processing is necessary for the performance of its official tasks carried out in the public interest in providing and managing a health service.

The PHA is the statutory regional organisation for health protection and health and social wellbeing improvement. The Health Protection Directorate provides strategic oversight and coordination of the implementation and ongoing delivery of regional vaccination programmes; provision of resources for health professionals and the public; interventions to improve uptake; disease and vaccine coverage surveillance; investigation, and management of cases, outbreaks and other immunisation incidents; and provision of expert advice to policy makers, commissioners, providers and the public.

In this instance the public task relates to the functions of the Public Health Agency which the Agency exercises on behalf of the Department of Health for:

> (a) the health improvement functions mentioned in subsection (2);
>
> (b) the health protection functions mentioned in subsection (3); and
>
> (c) obtaining and analysis of data and other information in subsection (4)
>
> as outlined in the Health and Social Care (Reform) Act (Northern Ireland), 2009, section 13.

The data collected on the Vaccination Management System includes personal data. Some of this data relates to health data which is described as 'special category data'. In relation to that processing, the following UK GDPR conditions apply:

- Article 9(2) (h) – the processing is necessary for medical diagnosis, the provision of health treatment and management of a health and social care system
- Article 9(2)(i) – the processing is necessary for reasons of public interest in the area of public health
- Article 9(2)(j) – the processing is necessary for archiving purposes in public interest – scientific/historical research purposes
- Data Protection Act 2018 Schedule 1, Part 1 (2) – Health or Social Care Purposes
- Data Protection Act 2018 – Schedule 1, Part 1 (3) – reasons of public interest in the area of public health
- Data Protection Act 2018 – Schedule 1, Part 1 (4) – reasons of public interest in the area of public health research

Common Law Duty of Confidentiality

Common Law is not written out in one document like Acts of Parliament, rather is it a form of law based on previous court cases decided by judges. The below illustrates how Common Law

Confidentiality requirements are met in relation to the processing of health data within VMS – it should be noted this list is not exhaustive:

- Staff working within the vaccination programme and collecting data for use within the analytics platform are governed by their professional codes of conduct and HSC contractual terms, including the duty of confidentiality.
- If information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. In practice, this means that all patient/client information, whether held on paper or computer, must not normally be disclosed without the consent of the patient/client.
- However, there are several very specific circumstances that make the disclosure of confidential information lawful, including the sharing of necessary information with other health and care professionals and agencies where the interests of patient safety and public protection override the need for confidentiality.
- The vaccination programme will need to share personal information in the interests of individual patient safety as the vaccination record held in VMS will need to form part of the individual's primary care record held by their General Practitioner.

5. VMS Risks Relating to Data

As with any project processing personal data, VMS carries several risks. These risks are examined in Appendix B, including the nature of any potential impact on individuals, rating likelihood and severity – together these form an overall risk rating. Appendix B also covers the responses VMS is putting in place to address and mitigate the risks as much as possible.

VMS accepts no risk mitigation is 100% effective – however the team, alongside taking advice from a variety of stakeholders in information governance and the Information Commissioners Office, is committed to addressing any risk which becomes an issue at a future point in time and will do so with diligence.

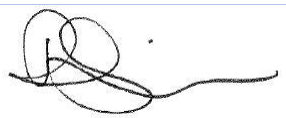
Prevention of Function Creep

When citizen vaccine information is collected and processed for one reason but is then used or processed in ways beyond the original VMS purpose this is called function creep. VMS is committed to minimising function creep during the requirements capture and design stage of any changes to VMS.

When VMS is required to share VMS data with any new external organisation or data processor an appropriate Data Sharing or Access Agreement (DSA or DAA) is put in place. These can only be approved by the Personal Data Guardian (or equivalent) within the data controller organisations once usage has been determined to satisfy data protection, confidentiality and appropriateness. This may also require the data controller organisations to consult with invested stakeholder groups prior to approval being given. This formal process ensures there is clear accountability and governance of the VMS during development and on-going operation to prevent function creep.

6. DPIA sign-off

Item	Name/position
DPIA reviewed and approved by:	(original VMS DPIA signed as below: Person 1 / Position – Legal Person 2 / Position – PHA Accountable Person 3 / Position – IG/PDG) This DPIA is an update, signed by PHA only as now including reference to CHS-VMS.
DPO advice provided:	Stephen Murray
Summary of DPO advice:	Previous versions of this DPIA relate to VMS only. This DPIA has been updated (v7.1) to include the adult pneumococcal programme. This DPIA has been updated (v7.0) to include the MenB programme for young people and remove details of NHS MESH usage which ceased in 2024. This DPIA has been updated (v6.9) to include the addition of access to data for research purposes through the HSCNI Honest Broker Service and reflect the reduction of external support. This DPIA has been updated (v6.8) to include the addition of pertussis and RSV vaccinations. This DPIA has been updated (v6.7) to include the closure of COVID Certifications Service, the addition of MMR vaccinations and the use of Google Analytics. This DPIA has been updated (v6.1) to include reference ONLY to the migration of data from CHS to VMS. Trusts aware and separate Data Sharing Agreement in place for CHS-VMS purposes. Any DPO comments are incorporated into this version. Previous VMS DPIA was updated to reflect PHA becoming sole Data Controller from 1 April 2023 (v5.0). Privacy Notice also updated to reflect revised Data Controllership from 1 April 2023.
This DPIA will kept under review by:	 **Dr Louise Herron** Deputy Director of Public Health Public Health Agency (PHA)

	 **Rachel Spiers** Senior Commissioning Lead - Immunisations Public Health Agency (PHA)

7. Appendix

Appendix A- VMS Stakeholder Landscape

Governance of VMS is provided by the VMS Board, chaired by VMS SRO and supported by the VMS Project Team. The VMS Board is made up of:

- Representatives from the vaccination programmes,
- Representatives from the end user community (Trusts, GPs and community pharmacy),
- Representatives from technology suppliers,
- Subject matter experts

For simplicity, the list below does not cover every stakeholder group, instead it represents those stakeholders who may at any point in time process VMS personal data:

- VMS Project Team – this team, staffed by PHA, maintains and delivers VMS.Technology Suppliers – these organisations deliver the technical aspects of VMS, commissioned by the VMS Project Team. Current suppliers are as follows, the first three are represented on the VMS Board:
    - BSO: provides first line support to VMS
    - Kainos: provides VMS recording platform
    - Aptvision: provides VMS booking platform
    - BHSCT: manages VMS Microsoft Azure hosting
    - Microsoft: provides hosting services
    - Google Cloud: provides hosting services
    - GOV.UK Notify: provides notification services
- Healthcare Providers – these organisations are the primary users of VMS, including both clinical (e.g. doctors) and nonclinical staff (e.g. administration teams).

Appendix B – VMS Data Risks

What are the risks?

Describe source of the risk and nature of potential impact on individuals		Likelihood of harm	Severity of impact	Overall Risk Rating
1	**Access by nominated VMS programme staff and developers to patient data** during product development cannot be limited, which may result in an unauthorised individual(s)/team(s) gaining access to sensitive data without having the necessary permissions.	Possible	Moderate	Medium
2	**Non-vetted staff users may exist** in the VMS accepted user lists	Possible	Moderate	Medium
3	**Risk of inaccurate data being entered into the VMS** by clinical staff or by members of the public that will delay the patient's vaccine booking and/or related activities. For example, - The ability to be able to stop a person booking into several different facilities to get their vaccines'. E.g. go to a Trust to receive first dose and then invited by GP for first dose. - Being able to overcome a common scenario where citizens are commonly known by one name but registered in Health and Care Index under another variation of this name. - The ability for citizens to obtain their COVID certification (COVID Certification Service ceased on 12th January 2024). - Incorrect citizens being contacted as part of the recall to be invited to receive their vaccine.	Possible	Minor	Low
4	**Risk of data loss during import of patient data from APTVision** solution to the Kainos VMS Dynamics data lake resulting in low quality, low confidence population. This will reduce the ability of the PHA to support the CMO in making timely decisions to accelerate and target vaccinations.	Remote	Moderate	Low
5	**Risk of data breach** (with the loss or unauthorised sharing of personal identifiable data, with potential impact of distress or reputational damage to individuals.), by staff working in the VMS Teams, through human error or intent. In addition, the risk of reputational damage to the PHA and DoH.	Remote	Moderate	Medium

6	**Risk of the VMS being 'hacked', with the theft of personal identifiable data** (data breach), with the risk of distress or reputational damage to individuals. Or the system being compromised or inaccessible because of a cyber security incident therefore VMS being unable to operate with no vaccine bookings being undertaken. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	Possible	Major	High
7	**Risk of unauthorised access (internal or external) to the personal data** on the VMS, APTVision (PostgreSQL), Kainos VMS Data (Azure Data Lake) and Reporting Platforms, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	Possible	Major	High
8	**Risk relating to Adult Safeguarding Privacy concerns,** particularly regarding inappropriate access to current information on identity and location. Vulnerable people may be particularly concerned about the risk of identification or the disclosure of information. Communication issues with vulnerable adults – issues with receiving/understanding information/instructions. If there are inadequate disclosure controls, there is an increase in the likelihood of information being shared inappropriately.	Possible	Major	High
9	**Risk of noncompliance with PHA/DOH data protection and information** governance policies and procedures which may result in accidental or deliberate misuse of sensitive personal data with potential of data protection requirements not being adhered to and for a data breach with the potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	Remote	Moderate	Medium
10	**Risk of noncompliance with established BSO ITS Service Transition Approval Process (**the VMS STAP) and the BSO do not have enough capacity to support the VMS. Potential, in error, to negatively impact the MS Dynamics environment and therefore the VMS would not be available when required.	Unlikely	Moderate	Medium
11	**Risk of access to personal data by 3rd party processors which may result in accidental or deliberate use of sensitive personal information.** Potential impact of a data breach, with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	Possible	Major	High
12	**Risk that personal data is used inappropriately for analytical purposes.** Inappropriate sharing of personal data which could result in potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	Rare	Minor	Low

13	**Risk of fraudsters sending similar looking messages with malicious intent.** Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, PHA and DHCNI.	Likely	Moderate	Medium
14	**Risk of fraudsters setting up a similar web booking front end** with malicious intent. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, PHA and DHCNI.	Possible	Moderate	Medium
15	**Risk of the VMS failing or suffering technical malfunctions rendering the system inoperable.** The impact of the VMS suffering failure would slow or reduce the vaccination programme's ability to vaccinate NI citizens.	Unlikely	Major	Medium
16	**Risk of data being shared with the wrong user/wrong users.** The impact of data being shared with the wrong individual would be that sensitive data would be shared incorrectly in addition to the risk of reputational damage and lack of trust in PHA from citizens.	Possible	Medium	Medium
17	**Risk of inaccurate data being entered into CHS** by clinical staff and transferred on to VMS. For example, - The ability to be able to stop a child attending a different facility to receive another vaccination. - Being able to overcome a common scenario where citizens are commonly known by one name but registered in Health and Care Index under another variation of this name.	Possible	Minor	Low
18	**Risk of data loss during import of patient data from CHS** to the VMS Dynamics data lake resulting in low quality, low confidence population. This will reduce the ability of the PHA to support the CMO in making timely decisions to accelerate and target vaccinations.	Remote	Moderate	Low
19	**Risk of data breach through use of GOV.Notify.** The impact of data being shared inappropriately or exposed would be that sensitive data would be shared incorrectly in addition to the risk of reputational damage and lack of trust in PHA from citizens.	Remote	Major	Medium
20	**Risk of data breach through use of Google Analytics.** The impact of data being shared inappropriately or exposed would be that sensitive data would be shared incorrectly in addition to the risk of reputational damage and lack of trust in PHA from citizens.	Unlikely	Major	Medium

What are the measures to reduce risks identified?

Describe source of the risk and nature of potential impact on individuals		Controls and measures in place to reduce risk	Effect on risk (Eliminated, Reduced, Accepted)	Residual harm (Low; medium; or high)
1	**Access by nominated VMS programme staff and developers to patient data** during product development cannot be limited	There are several controls in place and contractually suppliers covered under their contracts. Patient data processing and confidentiality is described and enforced by Kainos Limited's contractual and call-off terms under the UK's G-Cloud 11 & 12 framework agreements. Patient data and confidentiality is covered and enforces by APTVision contractual and call-off terms under the UK's G-Cloud 12 framework agreement. APTVision may process patient data on behalf of the controllers as a data processor for the purposes of development. No patient identifiable info in APTVision or Kainos pre-production environments.	Reduced	Low
2	**Non-vetted staff users may exist** in the VMS accepted user lists	A full user audit is carried out annually, all non-staff email addresses have been removed and no personal email accounts have access to VMS.	Reduced	Low
3	**Risk of inaccurate data being entered into the VMS** by clinical staff or by members of the public that will delay the patient's vaccine booking. For example, The ability to be able to stop a person booking into several different facilities to get their vaccines'. Go to a Trust to receive first dose and then invited by GP for first dose. Being able to overcome a common scenario where citizens are commonly known by one name but registered in Health and Care Index under another variation of this name.	Verification of patient identification via photo ID and checks against the HCN Index by vaccination staff conducted at the point of vaccination to mitigate data inaccuracies or errors made during phone or web bookings. Clinical staff have been briefed and trained on the use of the APTVision booking system and VMS Dynamics**.** The APTVision booking system has gone through numerous design changes to improve user experience, ease of use and accessibility to ensure patient entry errors are minimised. Once patient data has been entered into the VMS after the vaccine has been administered the record is 'locked'. Any subsequent changes to the record will need to be done via the VMS Service desk. Work was undertaken during operation of the COVID Certification Service (CCS) to monitor and improve data quality where data errors were noted at the point of checking vaccine data to administer certificates – CCS ceased on 12th January 2024.	Reduced	Low

4	**Risk of data loss during import of patient data from APTVision** solution to the Kainos VMS Dynamics data lake resulting in low quality, low confidence population. This will reduce the ability of the DHCNI to support the CMO in making timely decisions to accelerate and target vaccinations.	Automatic electronic import process is used to load the APTVision patient data extract on the Kainos VMS Dynamics data lake.	Eliminated	Low
5	**Risk of data breach** (with the loss or unauthorised sharing of personal identifiable data, with potential impact of distress or reputational damage to individuals.), by staff working in the VMS Teams, through human error or intent. In addition, the risk of reputational damage to the PHA and DoH.	All involved HSCNI staff in the VMS are required to complete the HSC information governance and IT Security e-learning module. • NI Direct has been established as the primary contact centre for the Northern Ireland Civil Service (NICS), its agencies and the wider public sector. • Suppliers to NI Direct must comply with Data Protection requirements and this is detailed in the contract with the supplier, in this case BT. The Privacy Notice is referenced at the start of each call. • There are strict protocols and training provided to the call handlers. The supplier also has a Quality Manager who sample checks calls against set criteria to score the call. • Risk and management of breach of confidentiality covered in training, in line with contract requirements. • Staff are subject to regulatory Codes of Conduct e.g., NMC and GMC which include duties of confidentiality. • Confidentiality clauses in contracts of employment of staff and supporting developer/advisory suppliers. • Appropriate disciplinary action will be taken in the event of proven breach • Staff operating within Trusts and GP Practices come under their respective IG governance rules and procedures.	Reduced	Low
6	**Risk of the VMS being 'hacked', with the theft of personal identifiable data** (data breach), with the risk of distress or reputational damage to individuals. Or the system being compromised or inaccessible because of a cyber-security incident therefore VMS being unable to operate with no vaccine bookings being undertaken. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	Kainos and Microsoft (VMS developers) comply with both international and industry-specific compliance standards and participate in rigorous third-party audits and penetration testing that verifies security controls. As required by the GDPR, the VMS developers implement and maintain appropriate technical and organisational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data it processes as a data processor or sub processor on its customers' behalf. APTVision meet the requirements of ISO 9001:2015 and develop/deploy their software products on the GDS approved G-Cloud provider Google Cloud. Google Cloud are Cyber Essentials certified and also ISO-27001, 27017 and 27018 certified. The VMS developers follow the UK Standard Contractual Clauses (data resides in secure cloud locations within the UK. The Belfast Trust (BHSCT) have applied the following security controls: ● Common data services is unavailable to everyone on WWW except for users within two Azure Active Directory groups ● Multi-Factor authentication is required to access the VMS outside of BHSCT Trusted locations (BHSCT and BSO Networks). ● Legacy authentication has been blocked for all users. ●A user must have a Dynamic 365 license assigned before they are able to access the Kainos VMS Common Data Services. ● Users will not be able to use the system unless added to an application role. ● Application roles have been set up to ensure a "least privileged" approach (Kainos developed). ● Only required accounts have been sync'd from on premise to Azure Active Directory via AD Connect.	Reduced	Medium

		APTVision security protocols include: ● Firewalls deny access by default ● Security patches applied automatically (nightly) ● All external traffic in transit encrypted ● SSL 2.0, 3.0, TLS 1.0, 1.1 are disabled, only TLS 1.2, 1.3 allowed ● No patient identifiable info in pre-production environments ● Certificates provided by DigiCert ● We have an A+ rating from Qualys SSL labs: https://www.ssllabs.com/ssltest/analyze.html?d=admin%2dimmunisation.aptvision.com&s=172.67.71.82&hideResults=on&latest ● HTTP Strict Transport Security (HSTS) used ● A recent external audit tested against OWASP top 10, all significant findings were resolved		
7	**Risk of unauthorised access (internal or external) to the personal data** on the VMS, APTVision (PostgreSQL), Kainos VMS Data (Azure Data Lake) and Reporting Platforms, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	Kainos and Microsoft (VMS developers) comply with both international and industry-specific compliance standards and participate in rigorous third-party audits and penetration testing that verify security controls. As required by the GDPR, the VMS developers implement and maintain appropriate technical and organisational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data it processes as a data processor or sub processor on its customers' behalf. APTVision meet the requirements of ISO 9001:2015 and develop/deploy their software products on the GDS approved G-Cloud provider Google Cloud. Google Cloud are Cyber Essentials certified and also ISO-27001, 27017 and 27018 certified. The VMS developers follow the UK Standard Contractual Clauses (data resides in secure cloud locations within the UK). **The Belfast Trust (BHSCT) & Kainos have applied the following security controls:** ● Common data services is unavailable to everyone on WWW except for users within two Azure Active Directory groups ● Multi-Factor authentication is required to access the VMS outside of BHSCT Trusted locations (BHSCT and BSO Networks). ●**Once logged into VMS, user actions are logged in an audit trail which includes CREATE, VIEW, UPDATE events on patient details** ●Legacy authentication has been blocked for all users. ●A user must have a Dynamic 365 license assigned before they are able to access the Kainos VMS Common Data Services. ● Users will not be able to use the system unless added to an application role. ● Application roles have been set up to ensure a “least privileged” approach (Kainos developed). ● Only required accounts have been sync’d from on premise to Azure Active Directory via AD Connect **APTVision controls** -APTVision sessions to the infrastructure (SSH access) records login time and IP source -Sessions to the admin portal are logged. There is auto logout functionality in place after session expires. -Once logged into VMS, user actions are logged in an audit trail which includes CREATE, VIEW, UPDATE events on patient details -Access to reporting functionality that includes export is controlled via individual user permission group that has to be explicitly assigned to selected users -SSH access require short lived (12 hour) SSH certificates, meaning regular re-authentication is required with the identity provider	Reduced	Low

		-Remote access is controlled using industry standard methods (SSH keys, no passwords allowed, secure VPN, roles and permissions assigned per user) **Kainos/Belfast Trust Controls** -All Belfast Trust Azure resources are managed via Azure Active Directory -Access to BHSCT Trust based Kainos Servers, Containers and Virtual Machines are restricted to via encrypted connection through Azure Bastion. Connection to Bastion is via whitelisted IP addresses only. Only named Azure Active Directory identities can access the DSVMs via this secure connection Security of VMS data as it moves from APTVision, into and within the VMS Kainos dynamics platform: - Data is securely transferred from APTVision to VMS via encrypted SSL/TLS connection using a secure Azure Logic App flow. A secure managed identity is used to connect the Logic App to Dynamics CRM which is associated with a least privilege security role granting the minimum permissions to update the VMS data model. -A named CRM service account with least privilege access is used in conjunction with a registered Azure Active Directory App to authenticate and authorise the data extract application when connecting to the Contact Tracing system to retrieve data for sync to the reporting database -This connection between the data extract application and Dynamics CRM web services is encrypted via SSL using TLS encryption -Future connections to PHA's Analytics platform - Azure Cosmos DB database will also encrypted via SSL/TLS and access is only granted via managed identity used by the Data Science VMs, reporting dashboard and data extract processes. I.e., there is no direct access to the database via a user of the Azure portal. This capability is not yet in place. Any VMS data stored in Cosmos DB will be encrypted at rest by default using AES-256 encryption.		
8	**Risk relating to Adult Safeguarding Privacy concerns,** particularly regarding inappropriate access to current information on identity and location. Vulnerable people may be particularly concerned about the risk of identification or the disclosure of information. Communication issues with vulnerable adults – issues with receiving/understanding information/instructions. If there are inadequate disclosure controls, there is an increase in the likelihood	Administration access to the VMS is controlled (as set out above), so no unauthorised personnel have access to the VMS. Only authorised clinical, Trust/GP administration and VMS development staff have access to the data on the VMS; they are bound by the existing controls and policies and professional regulatory Codes of Conduct. VMS operated by staff recruited for their professional skills (e.g., nursing) that will assist in communicating with vulnerable adults. In respect of vulnerable adults, the vaccinators and clinical staff will seek to speak to a proxy (e.g., legal guardian). If a vaccinator has a concern about the capacity of the contact, they can refer to the clinical lead. Managerial and clinical supervision arrangements are in place via the relevant Trust or GP Practice. Legal advice is sought as required.	Reduced	Low

	of information being shared inappropriately			
9	**Risk of noncompliance with PHA/ DoH data protection and information** governance policies and procedures which may result in accidental or deliberate misuse of sensitive personal data with potential of data protection requirements not being adhered to and for a data breach with the potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB, PHA and DHCNI.	Development of DPIA to identify risks & put appropriate measures in place; There is mandatory Information Governance and IT Security training; All staff have access to the DoH, PHA and DHCNI. Information Governance policies and procedures all available on each organisations intranet site; All staff bound by HSCNI employment contracts Staff bound by professional regulatory Codes of Conduct Appropriate disciplinary action will be taken in the event of proven breach.	Reduced	Low
10	**Risk of noncompliance with established BSO ITS Service Transition Approval Process (**the VMS STAP) and the BSO do not have enough capacity to support the VMS. Potential, in error, to negatively impact the MS Dynamics environment and therefore the VMS would not be available when required.	The VMS is being developed using a rapid, agile development technique which differs from a standard IT service transition used by the BSO. The VMS programme is collaborating with BSO, Suppliers and the BHSCT to align with the STAP process as closely as is practical to ensure a smooth transition to on-going sustainable services. Completion of documentation and approval by BSO ITS assistant director in line with existing governance applied to all HSC IT systems.	Reduced	Low

11	**Risk of access to personal data by 3rd party processors which may result in accidental or deliberate use of sensitive personal information.** Potential impact of a data breach, with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	No live system access rights are allocated to 3rd parties. All 3rd party access is in accordance with agreed contacts and contract management processes.	Reduced	Low
12	**Risk that personal data is used inappropriately for analytical purposes. Inappropriate** sharing of personal data which could result in potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, PHA and DHCNI.	All staff involved are HSCNI employees and therefore must comply with mandatory Information Governance training. Developers and advisory suppliers are bound by NDAs align with DHCNI Information Governance standards. Access to the Kainos VMS capability will be controlled via user management and allocation of appropriate rights and levels (e.g., read/write at various levels based on authorised need).	Reduced	Low
13	**Risk of fraudsters sending similar looking messages with malicious intent.** Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, PHA and DHCNI.	Advice was sought from the National Cyber Security Centre (NCSC) for VMS usage of SMS to ensure that the SMS is as safe as possible - this advice has been adopted when considering the use of NI Direct sourced SMS to confirm vaccine bookings. Sender ID based on guidance from the National Cyber Security Centre (NCSC) and SMS message content was also reviewed. Both have been classed as technically suitable by NCSC due to: The creation of some distance between SenderID and others nearby and the creation of a simple, recognisable link that is harder to mimic.	Maintained	Low
14	**Risk of fraudsters setting up a similar web booking front end** with malicious intent. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, PHA and DHCNI.	Advice was sought from the National Cyber Security Centre (NCSC) to ensure that the SMS is as safe as possible. There is a large amount of material available via website, apps etc. to ensure the public are fully aware of what information will be required and why.	Reduced	Low

15	**Risk of the VMS failing or suffering technical malfunctions rendering the system inoperable.** The impact of the VMS suffering failure would slow or reduce the vaccination programme's ability to vaccinate NI citizens.	The VMS Programme are adding the system to PHA's Information Asset (IA) Register. In the event of a major failure or catastrophe systems listed in the organisation's IA register are deemed critical and receive the highest priority in terms of resources and measures to restore back to normal operation. In such cases Trusts, GPs and other vaccination centres will revert to their existing patient records to ensure vaccination data is still captured during vaccine roll outs until the VMS has been fully restored.	Reduced	Low
16	**Risk of data being shared with the wrong user/wrong users.** The impact of data being shared with the wrong individual would be that sensitive data would be shared incorrectly in addition to the risk of reputational damage and lack of trust in PHA from citizens.	Access to the Kainos VMS capability is controlled via user management and allocation of appropriate rights and levels (e.g., read/write at various levels based on authorised need). All staff involved are HSCNI employees and therefore must comply with mandatory Information Governance training. Developers and advisory suppliers are bound by NDAs aligned with DHCNI Information Governance standards.	Reduced	Low
17	**Risk of inaccurate data being entered into CHS** by clinical staff and transferred on to VMS. For example, - The ability to be able to stop a child attending a different facility to receive another vaccination. - Being able to overcome a common scenario where citizens are commonly known by one name but registered in Health and Care Index under another variation of this name.	VMS treats CHS as the 'master record' for records sourced from CHS – any corrections made or records removed will automatically flow through to VMS. Records in VMS are clearly tagged as being sourced from CHS and are not editable in VMS. Any CHS data quality issues identified through VMS will be fed back to CHS for resolution.	Reduced	Low
18	**Risk of data loss during import of patient data from CHS** to the VMS Dynamics data lake resulting in low quality, low confidence population. This will reduce	An automatic electronic data transfer mechanism is used to convey records from CHS to VMS. All records transferred are identified by a unique CHS identifier. Any issues with the daily data transfer will be logged and notified to staff at the VMS provider, using the same methods implemented for transfer of HCN index data and data from other nations. Data transfer from CHS to VMS will occur on the HSCNI internal network, as with transfer from HCN index and to GP systems.	Reduced	Low

	the ability of the PHA to support the CMO in making timely decisions to accelerate and target vaccinations.			
19	**Risk of data breach through use of GOV.Notify.** The impact of data being shared inappropriately or exposed would be that sensitive data would be shared incorrectly in addition to the risk of reputational damage and lack of trust in PHA from citizens.	An automated data transfer mechanism via an FTP server is used to transfer data from NIHAP to the booking platform, in order for appointment booking templates to be created for citizens in the eligible groups, this reduces the likelihood of manual errors in transferring data. The booking platform then uses a second automated data transfer via the GOV Notify API to create the notifications to citizens, this again reduces the risk of manual errors. Access to both transfer mechanisms is limited to a small group of PHA, DHCNI and booking platform staff, and FTP access is locked down to specific IP addresses. The minimal dataset capable of supporting notifications is transferred. Data is transferred via secure protocols, it is not possible to pseudonymise data used for notifications. Only data for individuals deemed eligible for vaccination is sent in order to minimise the potential impact of any breach. In order to reduce the likelihood of distress caused by sending notifications to deceased citizens, notifications are only sent to individuals who can be identified by Health and Social Care Number and are therefore known, to the best available knowledge, to be living at the time the notification is requested.	Reduced	Low
20	**Risk of data breach through use of Google Analytics.** The impact of data being shared inappropriately or exposed would be that sensitive data would be shared incorrectly in addition to the risk of reputational damage and lack of trust in PHA from citizens.	The platform is configured so that it will not send form content to Google Analytics, so no personal information will be shared unless configuration errors are made. The configuration is reviewed as part of ongoing development of the platform and ongoing monitoring of Google Analytics (accessible by a small number of PHA staff). The use of Google Analytics is listed in the Privacy Notice, if citizens have opted out of all Google Analytics data sharing by blocking the required cookies then data from their booking platform sessions will be not be shared with Google Analytics.	Reduced	Low

Appendix C – Security Measures

Security measures are in place to ensure the information processed is carried out only as detailed in this DPIA and ultimately only for the purposes intended.

Relevant audit logs (in Aptvision and Dynamics) are in place, retaining a full audit history of both user access (who viewed what and when) and an audit history on field-level record modifications. The latter will record:

- The record that was changed,
- Who changed it,
- Timestamp,
- The value before the change,
- The value after the change for the affected fields.

Data processors meet the requirements of ISO 9001:2015 and develop/deploy their software products on the GDS approved G-Cloud provider Google Cloud. Google Cloud are Cyber Essentials certified and also ISO-27001, 27017 and 27018 certified.

The VMS developers follow the UK Standard Contractual Clauses (data resides in secure cloud locations within the UK). APTVision, Kainos and The Belfast Trust (BHSCT) have collectively applied the following security controls to protect the VMS:

- Multi-Factor authentication is required to access the VMS outside of BHSCT Trusted locations (BHSCT and BSO Networks). Legacy authentication has been blocked for all users.
- Common VMS data services are unavailable to everyone on WWW except for users within two Azure Active Directory groups
- APTVision sessions to the infrastructure (SSH access) records login time and IP source to track users access the APTVision system
- APTVision sessions to the admin portal are logged. There is auto logout functionality in place after session expires.
- Once logged into the tactical VMS, APTVision user actions are logged in an audit trail which includes CREATE, VIEW, UPDATE events on patient details
- Access to reporting functionality that includes export is controlled via individual user permission group that must be explicitly assigned to selected APTVision users
- SSH access require short lived (12 hour) SSH certificates, meaning regular re-authentication is required with the identity provider
- A user must have a Dynamic 365 license assigned before they are able to access federated VMS data and services.
- Application roles have been set up to ensure a “least privileged” approach (Kainos developed).

- Only required accounts have been sync'd from on premise to Azure Active Directory via AD Connect.

Vaccine Management Information Security

The organisational security measures implemented include the following security controls

- VMS citizen data can only be accessed under specific circumstance by authorised clinical/administration staff at GP practices, Trusts and Community Pharmacy Staff.
- Trust, GP staff and Community Pharmacy staff are nominated access by their role within their area of business only. Users will not be able to use the system unless added to an application role.
- Access controls for VMS vaccine administration staff is governed by each HSC Trust, GP Practice and Pharmacy operational procedures
- Access to citizen data is monitored by security and authentication mechanisms. Data access by clinical users, VMS administrators and development staff is also monitored and recorded for audit purposes.
- Common VMS data and analytic services are limited to specific users within two Azure Active Directory groups
- Only required accounts have been sync'd from on premise to Azure Active Directory via AD Connect.
- No live system access rights are allocated to 3rd parties. All 3rd party access is in accordance to agreed contacts and contract management processes.
- An appropriate separation of roles will be employed, for example developers will manage supporting backend configurations.

Security Controls in place for the VMS

VMS Suppliers Kainos, APTVision and Microsoft comply with both international and industry-specific compliance standards and participate in rigorous third-party audits and penetration testing that verify security controls. As required by the GDPR, the VMS developers implement and maintain appropriate technical and organisational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data they process as data processors or sub processors on its customers' behalf.

Both VMS Suppliers provide audit capabilities that allow the data controllers and processors to monitor vaccine data. VMS administrators can run a report on any patient record to see all the staff who have accessed it, what if any change were made and where that access was appropriate or necessary.

Appendix D gives more detail about the VMS security measures in place. A glossary at Appendix E gives more description of the technical terms and abbreviations.

How we control users who access the VMS and Reporting Platform

The organisational security measures implemented include the following security controls that have applied to the environment:

1. Restriction on user access to the VMS Reporting capability

    a) All Azure resources are managed via Azure Active Directory. This provides a mechanism to ensure only those who are on the system directory and authorised can access the VMS.
    b) Access to Data Science Virtual Machines is restricted to via encrypted connection through Azure Bastion. Connection to Bastion is via whitelisted IP addresses only. Only named Azure Active Directory identities can access the DSVMs via this secure connection
    c) Access to the Reporting dashboard is currently whitelisted to only Kainos IP addresses. When planning to open this up to HSCNI staff, it will be to named individuals identified by Azure Active Directory identity and whitelisted to the appropriate HSCNI IP addresses only.

2. Security of data as it moves into the strategic VMS and within the reporting platform is controlled by four mechanisms:

    d) A named CRM service account with least-privilege access is used in conjunction with a registered Azure Active Directory App to authenticate and authorise the data extract application when connecting to the VMS to retrieve data for sync to the reporting database
    e) This connection between the data extract application and Dynamics CRM web services is encrypted via secure method known as SSL which uses TLS encryption
    f) Connections to the VMS database[3] are also encrypted via SSL/TLS and access is only granted via managed identity used by the Data Science VMS, reporting dashboard, and data extract processes. I.e., there is no direct access to the database via a user of the Azure portal
    g) All data stored in the Azure DB is strongly encrypted using industry standards[4] All users are offered training to cover their use of the VMS. Training for the VMS to Trusts is provided on a 'train the trainer' basis and VMS run-throughs by the development team, video demonstrations and written manual.
    h) User readiness has been tracked as part Readiness meetings.
    i) GP and community pharmacy users are being supported by HSCB Practice Support Teams and DHCNI central team Further Developments

[3] Microsoft Azure DB

[4] At rest by default using AES-256 encryption.

As more information is made available about the different vaccines available in Northern Ireland the VMS may have to change and develop accordingly. While it is impossible to predict these developments at this stage several developments are anticipated including:

- VMS reporting function uses cloud architecture, hosted within Microsoft UK Southern Region datacentres, using software already configured within the Belfast Trust. In the longer term it will ultimately be re-provisioned centrally within Business Services Organisation when a Microsoft Azure environment for Northern Ireland can be constructed.
- Consideration of machine learning purposes, a human element would remain. There is no automated decision made by machines in this process, *all* decisions are human made. There are no plans to change this in the future.

As the Vaccine Management System DPIA is a living document it will be updated, as necessary.

Appendix D – Glossary

AD	Active Directory, which is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services
AES-256	The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
Azure	Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centres.
CHS	NI Child Health System
CMO	Chief Medical Officer who is the most senior government advisor on health matters.
COTS	Commercial off-the-Shelf Systems are products are packaged solutions which are then adapted to satisfy the needs of the purchasing organisation, rather than the commissioning of custom-made, or bespoke, solutions.
CRM	Customer Relationship Management system
Cyber Essentials	The Cyber Essentials certification was established by the National Cyber Security Centre (NCSC) in the UK to demonstrate that an organization has established safeguards to protect against the most common cyber threats.
Data Lake	A data lake is a system or repository of data stored in its natural/raw format. A data lake is usually a single store of data including raw copies of source system data, sensor data, social data etc.
DHCNI	Digital Health and Care Northern Ireland (DHCNI) is the data and technology lead to the Health and Social Care (HSC) system in Northern Ireland.
DLS	Directorate of Legal Services for Northern Ireland
DOH	The Department of Health for Northern Ireland
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment - this document.
G-Cloud	Is the principal commercial framework run by UK government for the purchase of cloud related software and services.
GDPR	This refers to the UK-General Data Protection Regulations
GDS	The Government Digital Service (GDS) which is part of the UK Cabinet Office. GDS's job is digital transformation of government.
GMS	General Medical Services is the term used to describe the very wide range of services and support that all patients receive from their General Practitioner (GP).
GP	General Practitioner commonly known as a Doctor
GPIP	GP Intelligence Platform. An aggregated platform that's still in development that takes data from the GP systems for sharing with other medical systems.
HCN	Health and Care Number. The HCN uniquely identifies a patient within the NHS in Northern Ireland. It is the equivalent of the NHS NUMBER in England and Wales.

HTTP	Hypertext Transfer Protocol (HTTP) is an application layer protocol for distributed, collaborative, hypermedia information systems
HSC	Health and Social Care
HSCB	The Health and Social Care Board (HSCB) is a statutory organisation that arranges or 'commissions' health and social care services for the population of Northern Ireland
HSCTs	Health and Social Care (HSC) Trusts in Northern Ireland. 5 HSC Trusts provide integrated health and social care services across Northern Ireland, the sixth is the NI Ambulance Service.
HSTS	HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking.
ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
IP	The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.
ISO 9001:2015	ISO 9001:2015 is an international standard dedicated to Quality Management Systems (QMS).
ISO 27001	ISO/IEC 27001 is an international standard on how to manage information security.
ISO 27017	ISO/IEC 27017 is a security standard developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security problems
ISO 27018	ISO/IEC 27018 is a security standard part of the ISO/IEC 27000 family of standards. It was the first international standard about the privacy in cloud computing services which was promoted by the industry.
ITIL	ITIL is a set of detailed practices for IT service management that focuses on aligning IT services with the needs of business
ITS	Information & Technology Systems
JCVI	The Joint Committee on Vaccination and Immunisation (JCVI) advises UK health departments on immunisation.
MS Dynamics	Microsoft Dynamics CRM is cloud based customer relationship management software package developed by Microsoft.
Multi-Factor authentication	Multi-factor authentication (MFA; encompassing Two-factor authentication or 2FA, along with similar terms) is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:
NCSC	National Cyber Security Centre (NCSC) is an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats.
NDA	Non-Disclosure Agreement
NIHAP	NI Health Analytics Platform, operated by HSC Data Institute

OWASP	Open Web Application Security Project (OWASP) is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security
PAC	The Privacy Advisory Committee whose role is to advise HSC bodies about the use of information relating to patients and clients.
PHA	Public Health Agency is the NI body responsible for health and social wellbeing, health protection, public health support to commissioning, policy and HSC research.
PostgreSQL	PostgreSQL also known as Postgres, is a free and open-source relational database management system (RDBMS) emphasising extensibility and SQL compliance.
SLA	Service Level Agreement which describes how a service will be delivered and defines the quality aspects of the service
SMS	Simple Messaging Service, also known as text messages.
SQL	Structured Query Language is a domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS).
SSH	SSH or Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.
SSL	Secure Sockets Layer (SSL) are cryptographic protocols designed to provide communications security over a computer network.
Subject	"Subject" refers to a person whose data is processed by VMS.
STAP	Service Transition Approval Process. This document provides BSO with the necessary information to take on support of a new healthcare Service.
TLS	The Transport Layer Security protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications.
VMS	Vaccine Management System used to support the delivery and roll out of vaccines across Northern Ireland