COVID-19 National Notification Service
System Security Policy (SSP)

Document control

Title	COVID-19 National Notification Service - System Security Policy (SSP)
Author	NHS National Services Scotland Information Security and Governance, Storm ID and Digital Health and Care Institute Scotland
Creation date	07/04/20

Version history

Version	Date	Comments
0.1	07/04/20	Initial Draft
1.0	28/04/20	NHS NSS Security and Architecture Review Board approved.
1.1	30/06/20	Amendments made to the document to move away from being a Negative Notification Service to a National Notification Service.

Table of contents

1 COVID-19 National Notification Service overview

1.1 Introduction

1.1.1 The Covid-19 National Notifications Service (NNS) is a new service being developed as part of the Digital Health and Care Institute's portfolio of responses to the current Covid-19 outbreak.

1.1.2 COVID-19 community testing services in Scotland are operating at maximum capacity in terms of testing patients and communicating results to tested patients within a forty-eight-hour period. A significant amount of time is spent in manual results lookup and contacting patients, and these activities have been identified as factors limiting testing capacity, leading to an increasing backlog of people waiting for test results.

1.2 Business goals/benefits of the system

1.2.1 The purpose of the Covid-19 National Notifications Service is to remove a significant burden of NHS effort spent manually notifying patients of Covid-19 test results using lists and telephones. Removing this task will free up capacity within the service and will allow it to carry out more tests per day.

1.3 System status and timescales

1.3.1 NNS is currently being developed by StormID for Health Protection Scotland, part of Public Health Scotland who also be the Data Controller for this service. The service will be deployed in an Internet-based digital platform currently hosted on NHS Greater Glasgow and Clyde ("NHSGGC") Azure infrastructure and used to provide digital services currently supporting NHSGGC COPD and Dermatology processes. (NNS will utilise components already deployed and make up the Lenus service that has SSP approval)

1.3.2 The Digital Health and Care Institute has initiated the project and is leading the early design and technical work with a view to handing the system to NHS Scotland to manage the commissioning and ongoing support and development of the service.

1.4 Privacy impact assessment

1.4.1 A DPIA is currently being produced by the Senior Consultant, Information Governance of NHS NSS (Information Security & Governance Pillar of Digital and Security Directorate)

1.4.2 The system resides entirely within the NHSGGC network and users/third parties cannot export data.

1.5 Responsible parties

1.5.1 The following individuals are responsible:

- System owner: NHS National Services Scotland
- System manager: StormID Ltd
- Senior information risk owner (SIRO): Deryck Mitchelson (Director of Digital and Security, NHS National Services Scotland).
- Information security officer/Accreditor: Head of Information Security, NHS NSS.
- Information governance officer: Senior Consultant Information Governance, Information Security & Governance, NHS National Services Scotland)

2 System description

2.1 Context

2.1.1 The Covid-19 National Notifications Service (NNS) is a new service being developed as part of the Digital Health and Care Institute's portfolio of responses to the current Covid-19 outbreak. PHS and NSS will be the Data Controller for this service. The service will be deployed in NHS Lothian and NHS Greater Glasgow and Clyde. These Boards will be Data Processors. Other Health Boards may adopt the service. Extending the service does not require new types of data to be processed.

2.1.2 The principal components and the virology data feed are all pre-existing technologies and services, and the practise of using SMS and email for outbound messaging to patients is also established in other services in NHSScotland.

2.2 Operation

2.2.1 The service hosted as Platform as a Services within Azure and operates as follows:

(a) The existing daily export file containing virology lab results is sent by the HPS 'ECOSS' system to an existing digital health platform (StormID Lenus) via the NHS NSS National Integration Hub (NIH) and the National Digital Platform (NDP)
(b) The NIH filters the virology input file to forward only Covid-19 specimen result information and the minimum associated patient data to the Lenus platform
(c) Patients are on-boarded to the service through a combination of automatic record creation in Lenus when virology results arrive for a patient who does not yet have a record, and manual input of patient contact information (SMS and email) obtained when the patient's test is being carried out.
(d) The algorithm in the Lenus platform records the specimen results for each patient
(e) The patient result is sent – via SMS and email if available – with a notification that they have a result to view. The result itself is not presented in the message.
(f) On opening the results page, an identity challenge is required before the patient is advised of their test result
(g) The service also includes a web application for NHS testing and administration staff to view the current status of patient results, providing sorting options to allow, for example, identification of patients who have been sent notifications but who have not yet accessed their results.

2.3 Hardware

2.3.1 (Architecture, summary of hardware, versions, configuration)

The NNS solution is hosted with the NSS Azure tenancy.

2.4 Software

2.4.1 (Server OS/platforms, versions of server and client software, thick or thin client, underlying/enabling technologies where appropriate (such as Java, .NET, php, etc.)

Azure Platform as a Service (PaaS) is used for infrastructure supporting the solution which means the Server OS and server OS level software is managed by Microsoft.

2.5 Interfaces

2.5.1 (List interfaces with other networks/systems/applications/organisations, describe how each communication and interface works e.g. SMTP email, web based access using SSL over HTTP, Internet facing web services based on WSDL, etc. Where possible capture specific technologies and versions of protocols in use)

- NNS Identity API requests/responses are made over HTTPS using TLS encryption.
- Patient API is authenticated with a patient specific identity token retrieved by the Patient App from NNS Identity. API requests/responses are made over HTTPS using TLS encryption.

- Email is sent from the Azure Functions using the cloud based email provider GOV.UK Notify for the sole purpose of sending email notifications to patients consisting of a short message including the patient's first name and a tokenized URL for the patient to access their National test result within the patient facing application. The token included in the URL is does not include and is not derived from any personal data assets.

  All requests are sent from Azure Functions over HTTPS using TLS encryption. Sensitive configuration settings for the integration with GOV.UK Notify are stored securely within Azure Key Vault.

  Email is also sent from Lenus Identity using Sparkpost for the following purposes:

  - Invitation emails for administrators added to the clinician facing application.

  - Password reset emails for administrators to rest their password.

  Email notifications are sent from the Azure Functions using the cloud based email provider SparkPost acting as an SMTP relay.All requests/responses are made over SMTP port 587 using TLS encryption. Sensitive configuration settings for the integration with SparkPost are stored securely within Azure KeyVault.

- SMS is sent from the Azure Functions using the cloud based SMS provider GOV.UK Notify sole purposes of sending SMS notifications to patients. HTTP requests are made to the REST GOV.UK Notify API to send SMS messages.

2.5.2

2.6 Accreditation scope

2.6.1 *(Summarise what is in scope and any scope exclusions)*

The accreditation scope should cover the components that make up the National Notification Service website, systems and processes. The scope would be as follows:

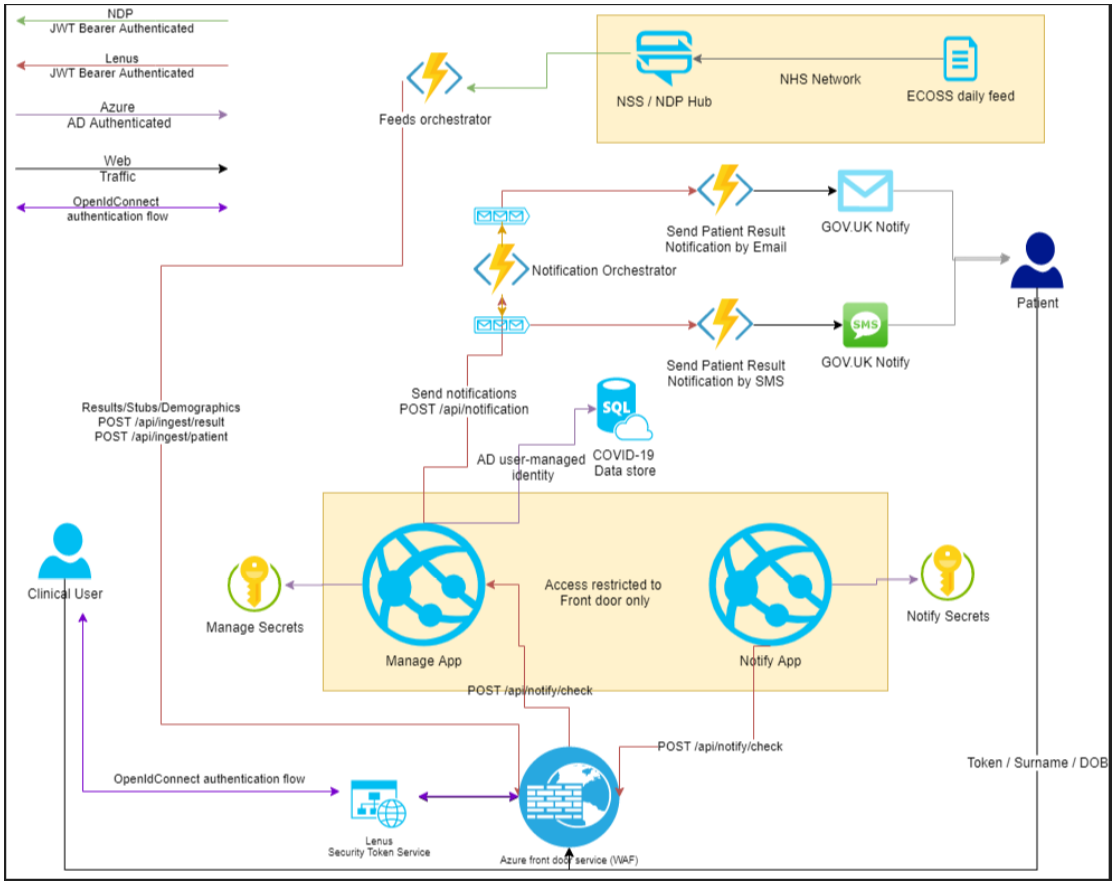
- Azure PaaS
- NNS Citizen Application
- NNS Clinical Application

Exclusions include the downstream components where NNS data is consumed these components are already covered by SSP accreditation of the Lenus system.

2.6.2 Figure 1 shows an overview diagram of the system.

2.6.3 All hosting of NNS is within Microsoft Azure Cloud the diagram in figure 1 shows components, data flow and security controls deployed within Azure.

Figure 1: diagram of proposed architecture


NDP
JWT Bearer Authenticated
Lenus
JWT Bearer Authenticated
Azure
AD Authenticated
Web
Traffic
OpenIdConnect
authentication flow
Feeds orchestrator
NSS / NDP Hub
NHS Network
ECOSS daily feed
Send Patient Result
Notification by Email
GOV.UK Notify
Notification Orchestrator
Patient
Send Patient Result
Notification by SMS
GOV.UK Notify
Send notifications
POST /api/notification
Results/Stubs/Demographics
POST /api/ingest/result
POST /api/ingest/patient
AD user-managed
identity
COVID-19
Data store
Clinical User
Manage Secrets
Access restricted to
Front door only
Notify Secrets
Manage App
Notify App
POST /api/notify/check
POST /api/notify/check
Token / Surname / DOB
OpenIdConnect authentication flow
Lenus
Security Token Service
Azure front door service (WAF)

3 Assets and services

3.1 Introduction

3.1.1 At the heart of a risk assessment are assets that are valuable to the business and need to be protected – these assets include:

- **Information assets** e.g. NHS data sets that must be protected from risks such as unauthorised access and loss
- **Physical assets** e.g. mobile devices or data centre equipment that must be protected from threats such as theft and fire damage
- **Services** e.g. clinical applications or infrastructure services like AD and DNS that must be protected from threats such as loss of service

3.1.2 This section captures the assets that are to be protected in the case of this information system.

3.2 Information assets

3.2.1 Table 1 lists the information assets.

ID	Name	Description	NHS sensitivity
A1	Patient personal and system login information	Patient title Patient first name Patient surname Patient date of birth Patient preferred name Patient sex Patient email address Patient residential street address Patient phone number CHI number **Note: In some cases, the point of contact may be a parent/guardian/carer/responsible adult for the patient.**	Red
A4	COVID-19 Test results	Patient COVID-19 test result is available to view within the NNS system.	Green
A5	Clinician System login details	Clinician username and password to authenticate to NNS for data read/write function	Red
A6	System Design	Design documentation listing components that make up the system	Green
A7	Source Code	Application Source Code	Green
A7	Azure Cloud Platform	Azure configuration and security settings	Amber

Table 1: information assets

3.2.2 The “NHS sensitivity” is the label applied to the information according to the NHS Scotland traffic light system as set out in Table 2.

Label	Description
Green	This is information which is unlikely to cause distress to individuals, breach confidence or cause any financial or other harm to the organisation if lost or disclosed to unintended recipients. This can include information which mentions only a person’s name (e.g. routine appointment confirmation letter) as long as it does not contain anything that is judged to describe a person’s physical or mental state.
Amber	In most boards the largest proportion of patient information can be said to require extra protection because it constitutes sensitive personal data as defined by the Data Protection Act. In particular:

Label	Description
	• any information about an individual (i.e. anything clinical or non-clinical) that would cause short-term distress, inconvenience or significant embarrassment if lost. • any information which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result). • any information if lost that would be likely to Nationally affect the efficiency of that service (e.g. cancellation of appointments).
Red	Most boards also hold some information which is highly sensitive. Particularly: • Any information which if lost could directly lead to actual harm (e.g. to mental health or put the person at physical risk from themselves or others in any way). • Any information that would in the opinion of a qualified person cause substantial distress and/or constitute a substantial breach in privacy (e.g. identity theft, loss of professional standing) to the subject. This is likely to include for example information on a person's sexual health. • Information that affects the privacy or could cause distress to more than one individual (e.g. several family members or several linked persons contained in a file). • Information relating to vulnerable persons' health (e.g. child protection cases) • Information governed by legislation that requires additional layers of security and recognises the substantial distress that would be caused by loss (e.g. embryology, human fertilisation and gender re-assignment). • Information if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

Table 2: NHS Scotland traffic light sensitivity descriptions

3.3 Physical assets

3.3.1 Table 3 lists the *major* physical assets comprising the system. (If it is a managed service and the supplier owns all the major physical assets this section can be omitted)

The systems and services are hosted within Azure Cloud.

3.4 Services

3.4.1 Table 4 lists the services provided by the solution.

ID	Name	Description	Max. tolerable downtime
S1	NNS Patient Interface	NNS application allowing patients to view COVID-19 test results	24 hours
S2	GOV UK Notify	Patient email and SMS notification system	24 hours
S3	SparkPost	Cloud email sending service	24 hours

Table 3: services

4 People

4.1 User groups

4.1.1 Table 5 lists the user groups with access to the system.

ID	Name	Description	Type of access	Number[1]
U1	Patients	COVID-19 patients awaiting test results	User read access	1000+
U2	Participating Health board Clinicians and testing teams	Input and process data	User read/write access	10 - 99
U3	Participating Health Board system support teams	Provide system support through diagnostics and repair	System Administrator	1 - 9
Non User Groups				
U4	Supplier Support	Service maintenance and support	Application administrator level access to source code	1 - 9
U5	Admin Support	Infrastructure support for Azure environment	Manage Azure tenancy.	< 5

Table 3: User groups

4.1.2 In addition to people based sources of threat the following non-people based sources of threat should be considered in the risk assessment:

4.2 Other sources of threat

4.2.1 In addition to people based sources of threat the following non-people based sources of threat shall be considered in the risk assessment:

- Environmental threats such as fire, flood
- Technical threats such as technical failure of equipment
- Automated threats such as worms that propagate mostly without human interaction

[1] Approximate number band: 1-9, 10-99, 100-999, etc.

5 Security controls

5.1 Supplier arrangements

5.1.1 What suppliers are involved in provision of any aspect of the solution? (identify all supplier groups including internal/health board teams, and external commercial third parties)

Storm ID – supplier of the COPD Service product

SparkPost – supplier of the email sending service

GOV.UK Notify – supplier of the email and SMS sending services

Microsoft Azure – used to host the solution

5.1.2 What contracts are in place? Summarise the information security/information governance/data protection contract terms, or other arrangements.

Microsoft Azure

Terms of Agreement

GOV.UK Notify

GOV.UK have a privacy notice available for Notify.

https://www.notifications.service.gov.uk/privacy

There are also terms of use available for the use of the GOV.UK Notify service.

https://www.notifications.service.gov.uk/features/terms

SparkPost

SparkPost provide a description of the subject matter, nature and purpose of their processing of personal data:

4.4.1 Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

4.4.2 Duration: As between SparkPost and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

4.4.3 Purpose: The purpose of the data processing under this DPA is the provision of the Service to the Customer and the performance of SparkPost pursuant to the Agreement (including this DPA) or as otherwise agreed by the parties.

4.4.4 Nature of the processing: SparkPost provides an email delivery, analytics, and intelligence service and other related services, as described in the Agreement.

4.4.5 Categories of data subjects: Any individual accessing and/or using the Service through the Customer's Account ("Users"); and any individual: (i) whose email address is included in the Customer's recipient list(s); (ii) whose information is stored on or collected via the Service, or (iii) to whom Users send emails or otherwise engage or communicate with via the Service (collectively, "Recipients").

4.4.6 Types of Customer Data:

i) Customer and Users: identification and contact data (name, address, title, contact details, username); financial information (account details, payment information); employment details (employer, job title, geographic location, area of responsibility);

ii) Recipients: identification and contact data (name, email address, and other demographic and segment data provided by Customer); IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data).

https://www.sparkpost.com/policies/dpa

SparkPost make assurances on technical and organisational measures taken to secure the personal data it processes in order to deliver services:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, SparkPost will implement and maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with SparkPost's security standards described at: https://www.sparkpost.com/policies/security ("Security Policy").

https://www.sparkpost.com/policies/dpa

SparkPost provides a complete list of all sub-processors, their location and their sub-processor activity.

https://www.sparkpost.com/policies/subprocessors/

5.1.3 Do information security requirements that apply to the named contractor also apply to any subcontractors? Name any sub contractors.

As Above

5.1.4 Who is responsible for reviewing supplier performance and ensuring conformance with security requirements?

Service Owner

5.1.5 What independent assurance/audits/certifications are applicable to any part of the solution? Describe the scope of any applicable certifications.

Storm ID certifications

Storm ID is Cyber Essentials Plus certified. The solution adheres to the five technical controls of Cyber Essentials:

- Secure your Internet connection
- Secure your devices and software
- Control access to your data and services
- Protect from viruses and other malware
- Keep your devices and software up to date

GOV.UK Notify certifications

Notify is certified to be used to send messages classified as 'OFFICIAL' or 'OFFICIAL-SENSITIVE' under the Government Security Classifications policy.

Formal risk assessments are carried out based on ISO 2700:2011.

Notify has been assessed and approved by the Cabinet Office Senior Information Risk Officer (SIRO). The SIRO checks this approval once a year.

Notify also has approval from the Office of the Government's SIRO to host data within the EEA.

The Notify team has Security Check (SC) level clearance from United Kingdom Security Vetting (UKSV).

SparkPost certifications

SparkPost has a Service Organisation Control (SOC) 2 Type II certification. This certification confirms that the SparkPost platform meets the strict information security and privacy standards for the handling of highly sensitive customer data established by the American Institute of Certified Public Accountants (AICPA).

5.2 Access control

5.2.1 How are new users provisioned? How is it ensured that users get the correct permissions?

Citizen provisioning

There is no permanent provisioning of citizen users in the traditional sense of having a login/password that persists.

A record is created for each citizen whose data is delivered into the NNS.

Citizens who have been tested for Covid-19 and whose test results are presented into the NNS are sent a message in an SMS text and/or email to the contact information they provided at the time of their test. The link is unique to that citizen. When activated by the citizen, the link takes them to a private page on the NNS citizen app. An identity challenge is presented to confirm the citizen is authorised to view the test result. If the challenge is passed, the citizen will be able to view their notification details. The link will persist while the notification is active to allow the citizen to access their results again should they wish. Notifications will be superseded by subsequent notifications for the same patient, meaning that the link for the previous notification will no longer be valid.

Each new test on a citizen will follow the same process, with a unique link being generated each for each additional test result.

Clinical dashboard user provisioning

Users are provided with a login account to the Lenus platform which is accessed via the clinical dashboard application.

For each Health Board, a 'superuser' will be nominated by the Board. The superuser account will be created by Storm. The superuser account is created with a fixed set of privileges, which is the set of information search, view, update privileges that are accorded to all clinical users, with the addition of the capability to add or remove clinical users for their own Health Board domain only.

Additional clinical users will be provisioned (and removed from the system when required) by the superuser.

For all non-superuser accounts, the privileges are granted the same: there is only one 'profile', with the exception that clinical users are able to access only the patient information from their own Health Board.

5.2.2 How do users log onto the solution? Are there different options for different interfaces?

Citizens

Citizens do not have permanent user accounts with a log-in. Users access their test results via a challenge on the citizen-facing web application (challenge is first name and DoB), which they reach using the unique link that is sent to them by text/email.

A fresh link is sent for each test result if the patient is tested more than once.

This is the only route for citizens to access the service.

Clinical dashboard users

Clinical dashboard users have a dashboard 'landing page' which presents the login challenge and on successful progression past the challenge the dashboard screens are accessed.

There is only one route for clinical dashboard users to access the system.

5.2.3 How is it ensured that users can only access the information and functions for which they are authorised?

There is only one route for citizens to access the service, and the functionality of the citizen-facing service is determined by the application.

There is only one route for clinical dashboard users to access the system. The access rights are managed within the clinical dashboard application.

5.2.4 How are the user accounts managed? For example, who removes accounts of staff that leave the organisation, resets forgotten passwords, updates a users permissions, changes to permissions, etc?

For each Health Board, a 'superuser' will be nominated by the Board. The superuser account will be created by Storm. The superuser account is created with a fixed set of privileges, which is the set of information search, view, update privileges that are accorded to all clinical users, with the addition of the capability to add or remove clinical users for their own Health Board domain only.

5.2.5 How can users recover their account if they forget their credentials?

Citizens

This is not a requirement for citizen access.

Clinical dashboard users

Clinical users can complete the password request flow if they have forgotten their password.

5.2.6 How are user credentials, such as passwords, stored within the system?

Clinical dashboard users

They are not stored within the system, they are managed using Lenus Identity.

5.2.7 Are any individuals/groups, who are **not** authorised users of the system, able to access any part of the system e.g. the hardware or shared infrastructure components? (For example cleaners or patients that may be able to access physical terminals in shared areas; or users of other applications that may be able to access a shared database or hosting environment)

No.

5.3 Personnel controls

5.3.1 What personnel pre-employment screening checks are applied for personnel involved in provision of the service?

Storm ID personnel controls

Storm ID carry out background checks on all staff to ensure that Storm ID:

- have verified their identity
- have confirmed their right to work in the UK status
- have verified their employment history and qualifications
- have confirmed they have no unspent convictions (Basic Disclosure)

Clinical Support Staff

All clinical staff go through standard HR recruitment processes which includes identity verification and other checks as necessary for the actual position.

5.3.2 How are users made aware of their security responsibilities with respect to the system? (e.g. to keep their password secret, or to report a security breach?)

Citizens

For citizens accessing their test results there is no specific guidance given as there is only a read only function within the application to view test results.

Clinical dashboard users

NHSS users of the clinical dashboard application are already subject to training on information safe handling, and the use of the clinical dashboard application falls within the scope of their existing briefings and training on the secure use of information systems.

5.3.3 What training is provided to system administrators or managers on how to properly run the system?

The solution is managed by Storm (ID) Ltd (SC216070) as System Operator. The Storm support team also supports other NHSS systems on the Lenus platform, e.g. NHS GGC COPD and Dermatology appointments service. The general principles and procedures that apply to other NHSS systems also apply to the National Notifications Service, e.g. managing tickets, problem recording, investigation and resolution.

5.3.4 What information security and governance training is provided to users of the system?

NHSS users of the clinical dashboard application are already subject to training on information safe handling, and the use of the clinical dashboard

application falls within the scope of their existing briefings and training on the secure use of information systems.

5.4 Network security controls

5.4.1 Are the system's network interfaces hardened? For example, have all unnecessary services been disabled and ports closed?

Yes.

5.4.2 How does the solution protect access to network traffic on shared networks?

The solution is deployed to the Azure public cloud where it does not have any access to network traffic on shared networks. Solution components that integrate with other systems are protected with both application level and network level security to prevent unauthorised network access to the destination infrastructure.

5.4.3 How is the hosting environment separated/protected from connected networks (e.g. firewall(s), models, config, etc.)?

See answer above

5.4.4 Have all network components been deployed in a hardened configuration, for example all default passwords changed, and unneeded services blocked?

5.4.5 Yes

5.4.6 Is the solution remotely accessible? If so, how is the remote access provided and controlled?

The solution is remotely accessible via the Azure management portal. Access is strictly controlled with only those permissions required to carry out solution and infrastructure maintenance being granted with role-based access control and under change control agree by the relevant CAB.

5.5 Data protection

5.5.1 Who are the data controllers and data processors for this solution?

HPS are data controllers for the test result data within ECOSS.

NHS GG&C and NHS Lothian are also Data Controllers of data relating to patients accessing NHS care within their territorial NHS board geographical areas.

Territorial Health Boards whose testing teams use the service, do so to:

- Input patient contact information (telephone number and email address)
- View patient test results status (positive, negative, and whether a patient has accessed their result).

The territorial Boards using this service and providing additional data feeds through Trak are also Data Controllers for the data pertaining to their own patients.

NSS, as a Data Controller will operate the service on behalf of NHSScotland Boards

National Integration Hub (NIH). The NIH receives incoming data feeds from the PHS ECOSS service. This contains patient, HB, and laboratory test result information that is processed and filtered by the NIH for onward transmission of COVID-19 results to the Storm Lenus platform.

NHS National Education Scotland Digital Service is a Data Processor for the data that transits from the NIH to the Storm Lenus platform via the National Digital Platform (NDP).

Storm ID is a data processor for the data that is ingested into the Storm Lenus platform via the NIH and NDP.

Microsoft is a data sub-processor for the infrastructure supporting the Storm Lenus platform and NNS solution.

5.5.2 Are all information assets held in the system allocated to a responsible owner?

Yes. The IG Rapid Assessment Form lists the Data Controllers and Data Processors for the information assets.

The data in the Lenus platform that relates to citizens is owned by the citizens themselves (Assets A1 and A4 where these relate to individuals).

Clinician login information (Asset A5) is owned by the employing Health Board.

System design documentation (Asset A6) is owned by Storm ID.

Source code (Asset A7) is owned by Storm ID

The Azure cloud service (Asset A8) is owned by NHS GGC (at time of publication of this SSP, Marie Farrel is the named owner on behalf of NHS GGC).

5.5.3 Are any technical controls employed within the solution to protect information assets? For example, encryption at rest, de-identification or data obfuscation.

All information assets are encrypted at rest and in transit. Dynamic Data Masking is also applied to Azure SQL databases to mask and de-identify stored data.

5.5.4 What controls are in place to ensure secure disposal of hardware and information assets? For example, to prevent unauthorised recovery of data on recycled hard disks, or secure shredding of printed output.

The NNS platform is deployed on the NHSGGC Azure tenancy so is subject to Microsoft's standard Azure terms and conditions relating to disposal of hardware. Data processed by individual Health Boards should be handled based on local Data Protection policy.

5.5.5 How is data imported/exported from the solution? What controls are employed to protect any data on removable media?

Participating Health Boards, Data Protection and removable media local policy should apply.

5.5.6 What information transfers does the solution permit/enable? How are these controlled?

Data flow and associated controls within the service are described in the figure within section 2.6.2. The text below outlines patient and clinical users journey,

1. A Clinical user will access the clinical management app in order to "Add a new patient test" (note that a single patient may be tested multiple times). The clinical user will complete a series of demographic fields relating to the patient including: Name, DOB, Mobile Number, Email and CHI (retrieved from Trak)
2. When the patient test is created, it will be stored centrally within the COVID-19 data store, this will be referred to as a "patient test stub" as it is yet to contain a test result, only the intention to test. The creation of this will initiate an orchestration that will begin and wait for receipt of a test result via the "Inbound FHIR message receiver" (3).
3. The "Inbound FHIR message receiver" will accept messages from NSS/NDP containing a negative or positive test results related to COVID-19, these will be parsed and reconciled against existing "patient test stub" records within the COVID-19 data store. This reconciliation will append the test result to the "patient test stub", thus completing the test record. IN the case that a patient record stub does not yet exist but a test result is received we will create a patient test stub with the test result information and flag these to clinical users via the interface and a specific status.
4. When a "patient test stub" is reconciled and completed the "Notification Orchestrator" will continue by sending outbound SMS and email notifications to the patient associated with the test record
5. The patient will follow a link within the SMS or email notification to visit the notification web app where they will be requested to input their surname and date of birth for identity verification.
6. The patient's surname and birth of birth, along with a unique token that formed part of the URI will be passed to a test retrieval endpoint. If a result is found matching the verification values it will be returned and displayed to the patient, otherwise a message will be displayed to inform them that no result was available
7. Once the test result is displayed to the patient an acknowledge request will be sent to another endpoint, this will update the test record status in order to inform the clinical team that the patient reviewed their test result
8. Patient test records and statuses will be displayed and updated within the clinical app interface

5.6 Physical and environmental security

5.6.1 What physical or environmental controls apply at any locations where the solution is hosted?

Storm ID defer to the Azure physical security policy for solutions hosted in Azure.

https://docs.microsoft.com/en-us/azure/security/azure-physical-security

The Azure infrastructure is designed to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. It also meets country-specific standards, including UK G-Cloud. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

5.6.2 What physical security controls apply at any locations from where the solution is used/accessed?

Storm ID physical security controls

Our physical security policy applies to all forms of physical security relating to Storm's offices, including:

- Buildings - including entry and exit points and windows
- Secure rooms - such as computer rooms
- Computer equipment - both inside and outside the office
- Documents - hardcopies
- People - staff, guests and contractors

Audits take place every 6 months to assess the current situation, find out what has changed since the last audit, and make recommendations for updates to the policy and process. These audits involve a review of the risks. There is limited access to the computer rooms, which required both a key and knowledge of the passcode to enter.

Participating health boards local physical security policy should apply.

Participating Health Boards computers used by staff are protected by standard security measures governed by local security policy.

5.7 Operational security

5.7.1 Who is responsible for Information Backup controls? Describe the data backup and recovery process.

Storm ID's IT team are responsible for maintaining Information Backup controls.

All business-critical data is backed-up and restores are tested on a schedule.

All data held within backup and DR environments is provided the same security and protection as data held in live data stores.

Where possible, cloud resources of any kind are geographically housed and/or replicated, across multiple regions, to provide a highly available solution.

In the case of data stores – Storage or Database (both of which will be designed in a Highly Available fashion) – regular snapshots of data, built-in 'Point-in-time-Recovery' up to 35 days, and fully customisable long-term retention policies of both, offer a unique software-defined backup and DR solution for any application.

Azure Devops CI/CD pipelines, including templated Infrastructure as Code (IaC) ensures that, in the case of Disaster Recovery, both infrastructure and application code can be redeployed to a previously known and working state in minutes.

DR scenarios and RPOs/RTOs are factored into solutions where necessary.

5.7.2 Who is responsible for solution Change Management? Describe the change management process.

Storm ID change management

The project manager is responsible for change management.

All changes to systems are properly tested and authorised, and Storm ID make use of technologies such as ARM templates to prevent unauthorised changes.

Changes to integration components of the solution are managed through the GGC change management process. Where such changes also require change to components in the main applications, the National Digital Platform or the National Integration Hub, they are coordinated through the GGC innovations team using the GGC change management process and feed into the individual change management processes that each downstream organisation has in place

5.7.3 What anti-malware controls apply within the solution?

No files are currently submitted by any users of the solution. The use of Azure Platform as a Service (PaaS) infrastructure also obviates the risks associated with malware that would be present if Infrastructure as a Service infrastructure (IaaS), such as Virtual Machines, was in use.

5.7.4 How are information security incidents (or potential information security incidents) reported, managed and communicated?

Storm ID information security incident management

Storm ID has policies and procedures in place for reporting and investigating breaches of security. All users of the Storm's IT facilities and physical information are required to understand and use these policies and are responsible for helping to ensure the safety and security of our systems and the information that Storm ID use or manipulate.

Storm ID has systems in place for monitoring and alerting to help us identify and investigate information security incidents.

Storm ID undertakes risk assessments to identify, quantify, and prioritise risks. Controls will be selected and implemented to mitigate the risks identified.

Information security incidents definition and process

An information security incident occurs when there is an event that has caused, or has the potential to cause:

- Damage to the organisation's information assets.
- Damage to the organisation's reputation.
- The corruption of data.
- The unauthorised transfer of data or information to someone who is not entitled to receive it.

An Information Security Incident includes:

- The loss or theft of data or information both physical and electronic
- The transfer of sensitive or confidential information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system from inside or outside Storm.
- Changes to information or data or system hardware, firmware, or software characteristics without the organisation's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system by any person.
- Loss of service.
- System malfunctions.

All events and suspect events that could result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems must be reported immediately.

The Operations Director and/or Technical Director must be contacted by email to dataprotection@stormid.com, telephone or in person. They will record the incident using the report a security incident form and notify relevant employees and the information owner. If the Operations Director

and/or Technical Director is unavailable, then another director should be contacted.

The Operations Director and/or Technical Director will require further information to be supplied by the person who has identified the incident, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Name of person reporting the incident
- The type of data or information involved (be it electronic or physical)
- Whether the loss of the data puts any personal or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of information or equipment affected
- Type and circumstances of the incident

The Operations Director and/or Technical Director will notify the information owner and escalate the incident to the appropriate responsible person as defined in the risk impact matrix.

Serious incidents should be reported to the Directors immediately.

Storm ID shall notify the controller within 1 working day of the event where data or system may be defined as business sensitive, personal, personal sensitive, personal identifiable or special category data. Other data sets will be reported within 3 working days.

The notification shall include the same information as would report for a data breach if Storm ID were the data controller.

The notification will be supplied using secure channels.

5.7.5 What controls have been employed to ensure continuity of service?

Storm ID continuity of service controls

Storm ID maintain and test business continuity plans that include scenario planning and procedures to be followed in the event of a serious emergency (for e.g. an office fire) to enable us to deliver an uninterrupted service.

This includes planning for:

- Mobilisation of incident management team
- Temporary office relocation

- Remote home working
- Access to financial reporting
- Communications, command and control procedures
- Cloud SaaS services and internet access

5.7.6 Has a business continuity plan and a disaster recovery plan been produced for the solution? Have these plans been tested?

As above.

5.8 Audit controls

5.8.1 Describe the audit controls employed by the solution. What events are recorded? For how long are audit logs retained? What tools are available to analyse audit logs?

Audit controls employed by the solution

The solution has database audit controls in place which audit database events and queries for the SQL database within the solution. The audit logs are stored in Azure storage.

Audit controls for Storm ID employees

The following are the audit controls that are in place within Azure for authorised Storm ID employees:

- User ID's
- Dates
- Times
- Key events such as long on/off
- Searching for records
- Reading of records
- Printing of records
- Terminal ID
- Successful and rejected system access attempts
- Use of privileges
- Changes to system configuration

Azure Log Analytics will provide centralised logging, which can include these records for both on-premises and cloud-based resources.

The system is configured to retain audit logs for at least 6 months.

Azure Log Analytics will provide centralised logging, which can include these records for both on-premises and cloud-based resources.

5.8.2 Who is responsible for auditing system access?

Storm ID auditing responsibility

Storm ID IT manager has responsibility for auditing system access and notifying of, and/or acting upon suspicious or unusual activity for Storm ID employees.

5.8.3 How are audit logs protected from unauthorised access or modification?

The use of Immutable azure storage to store assets and case related documents in accordance with regulatory compliance SEC 17a-4(f), CFTC 1.31(d) and FINRA allows for legal hold and time-based retention policies to be assigned to documents and other assets within storage account.

Immutable secure document retention ensures that data cannot be modified or deleted by any user, including those with administrative access.

Azure Advanced data security (ADS) provides a set of advanced SQL security capabilities, including data discovery and classification, vulnerability assessment, and Advanced Threat Protection.

- Data discovery and classification provides capabilities built into Azure SQL Database for discovering, classifying, labelling and protecting the sensitive data in databases. It is used to provide visibility into database classification state, and to track the access to sensitive data within the database and beyond its borders.

- Vulnerability assessment is a service that discovers, tracks, and helps remediate potential database vulnerabilities. It provides visibility into security state, and includes actionable steps to resolve security issues, and enhance database fortifications.

- Advanced Threat Protection detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. It continuously monitors database for suspicious activities, and provides immediate security alerts on potential vulnerabilities, SQL injection attacks, and anomalous database access patterns. Advanced Threat Protection alerts provide details of the suspicious activity and recommend action on how to investigate and mitigate the threat.

Azure Policy is tailored to detect inconsistencies with defined infrastructure configuration baselines and best practices and ensure that resources stay compliant with corporate standards.

Customisable alerting is available across each of these complimentary Azure governance-based resources.

5.9 Solution development, testing and maintenance

5.9.1 Who is responsible for deploying patches and updates?

Storm ID developers and members of Storm ID's Web Operations team are responsible for deploying updates to the deployed applications. The use of PaaS infrastructure means that Microsoft Azure is responsible for the patching of server operating systems.

5.9.2 In what timescales will patches and updates be deployed?

Application updates are deployed regularly based on an agile development release cycle that ranges between one deployments every two weeks to one deployment every month. High priority updates, such as security related updates, are prioritised and deployed within 3 working days.

5.9.3 Are any components of the solution **excluded** from the above patching policy?

The Lenus Identity application is updated on a separate but similar release cycle and update policy which ranges from one deployment every month to one deployment every two months. High priority updates, such as security related updates, are prioritised and deployed within 3 working days.

5.9.4 Describe the patch deployment process.

A build producing a deployment artefact runs in Storm ID's continuous integration environment once a code pull request has been completed and approved following technical peer review.

Continuous deployment to the development environment is automated and triggered automatically by the completion and approval of the pull request.

The automated deployment of a release artefact to the test environment requires manual approval by a tester (a member of the Storm ID Quality Assurance team). Once internal QA testing has been completed for a release on the development environment.

After an automated deployment to the test environment has been completed, automated deployment of the same artefact to the production environment require approval by at least one tester and then, in sequence, subsequent approval by at least one member of the Web Operations team.

5.9.5 What testing controls are in place to understand any potential unintended impacts of updates?

5.9.6 Storm ID application testing includes:

- Functional testing

- Regression testing
- Browser and device testing
- Exploratory Testing
- Performance testing
- Security scanning testing
- Security Penetration testing

5.9.7 What agreements are in place to ensure the solution keeps pace with information security developments? For example migrating onto new information technologies when previous versions become obsolete/unsupported.

The solution is cloud-based, so security updates are part of the service provided. Storm ID also use security and vulnerability scanners throughout the product lifecycle to actively seek out and fix vulnerabilities in the system such as out of date software versions.

5.9.8 What security testing has been performed on the solution? What was the outcome of the test? What commitment has been made to ongoing security testing? (this may include things like an IT Health Check on servers, a pen test on external interfaces, vulnerability scans on the servers)

5.9.9 Commissum Cybersecurity were commissioned to undertake a penetration test of the NNS application and associated relevant interfaces.

StormID used Detectify, a third-party website vulnerability scanner was used throughout the product lifecycle on a scheduled basis and on deployment to test for OWASP Top 10 including SQL, LDAP, XPATH and NoSQL injections, Cross Site Scripting flaws, broken session management, remote code and command execution, malware, etc.

5.9.10 Is there a separate test and development environment? Is any live data utilised in this environment? How is access to the test and development environment controlled?

Yes, there are separate test and development environments. No live data is used in any of the test or development environments.

5.10 Assumptions

5.10.1 What assumptions have been made about security controls that are out of scope of this SSP? For example, assumptions about controls that are believed to be the responsibility of the health boards or suppliers such as end user device security, behaviours or responsibilities, physical/environmental security at operating locations, etc.

It is assumed that:

- the physical and environmental security of Azure data centres is the responsibility of Microsoft and is out of scope for this SSP
- the security of end user devices used to access the solution are the responsibility of the end user and is out of scope for this SSP

6 Risk analysis and recommendations

This section to be completed in collaboration with the Accreditor/information security practitioner.

6.1 Residual risk statement

6.1.1 Table 6 provides a summary of the key residual risks identified.

6.1.2

Table 4: Summary of key risks

6.2 Risk treatment recommendations

6.2.1 Significant residual risks

- From information provided within the SSP, no significant residual risk to be accepted.

6.2.2 Risk treatment

- Data restoration tests to be carried out to ensure the integrity of the platform following an adverse event.

6.2.3 Accreditation recommendation

- Annual review is suggested. (StormID should re-engaging with IS&G to assess platform status on a yearly basis.)

6.2.4 System Security Policy approved.

7 Annex A – NHS Scotland risk matrices

7.1 Impact/consequence definitions

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Patient Experience	Reduced quality of patient experience/clinical outcome not directly related to delivery of clinical care.	Unsatisfactory patient experience/ clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience/ clinical outcome; short term effects – expect recovery <1wk.	Unsatisfactory patient experience/ clinical outcome; long term effects – expect recovery >1wk.	Unsatisfactory patient experience/ clinical outcome; continued ongoing long term effects
Objectives / Project	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope or quality of project; project objectives or schedule.	Significant project over-run.	Inability to meet project objectives; reputation of the organisation seriously damaged.
Injury (physical and psychological) to patient/visitor/staff.	Adverse event leading to minor injury not requiring first aid.	Minor injury or illness, first aid treatment required.	Agency reportable, e.g. Police (violent and aggressive acts). Significant injury requiring medical treatment and/or counselling.	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.	Incident leading to death or major permanent incapacity
Complaints / Claims	Locally resolved verbal complaint.	Justified written complaint peripheral to clinical care.	Below excess claim. Justified complaint involving lack of appropriate care.	Claim above excess level. Multiple justified complaints.	Multiple claims or single major claim Complex justified complaint.

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Service / Business Interruption	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service.	Short term disruption to service with minor impact on patient care.	Some disruption in service with unacceptable impact on patient care. Temporary loss of ability to provide service.	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.	Permanent loss of core service or facility. Disruption to facility leading to significant “knock on” effect
Staffing and Competence	Short term low staffing level temporarily reduces service quality (< 1 day). Short term low staffing level (>1 day), where there is no disruption to patient care.	Ongoing low staffing level reduces service quality Minor error due to ineffective training/implementation of training.	Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training/implementation of training. Ongoing problems with staffing levels.	Uncertain delivery of key objective/ service due to lack of staff. Major error due to ineffective training/implementation of training.	Non-delivery of key objective/service due to lack of staff. Loss of key staff. Critical error due to ineffectivetraining/ implementation of training.
Financial (including damage / loss / fraud)	Negligible organisational/personal financial loss. (£<1k). (NB. please adjust for context)	Minor organisational/personal financial loss (£1-10k).	Significant organisational/personal financial loss (£10-100k)	Major organisational/personal financial loss (£100k-1m).	Severe organisational/personal financial loss (£>1m).
Inspection / Audit	Small number of recommendations which focus on minor quality improvement issues.	Recommendations made which can be addressed by low level of management action.	Challenging recommendations that can be addressed with appropriate action plan.	Enforcement action. Low rating. Critical report.	Prosecution. Zero rating. Severely critical report

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Adverse Publicity / Reputation	Rumours, no media coverage. Little effect on staff morale.	Local media coverage – short term. Some public embarrassment. Minor effect on staff morale/public attitudes.	Local media – long-term adverse publicity. Significant effect on staff morale and public perception of the organisation	National media/adverse publicity, less than 3 days. Public confidence in the organisation undermined. Use of services affected.	National/international media/adverse publicity, more than 3 days. MSP/MP concern (Questions in Parliament). Court Enforcement. Public Inquiry/ FAI.

Table 5: Impact/consequence definitions

7.2 Likelihood definitions

Descriptor	1 Very low (VL)	2 Low (L)	3 Medium (M)	4 High (H)	5 Very high (VH)
Probability	Rare - can't believe this event would happen – will only happen in exceptional circumstances	Unlikely - not expected to happen but definite potential exists – unlikely to occur.	Possible - may occur occasionally, has happened before on occasions – reasonably chance of occurring	Likely - strong possibility that this could occur – likely to occur	Almost certain - this is expected to occur frequently / in most circumstances – more likely to occur than not

Table 6: Likelihood definitions

7.3 Risk matrix

	Impact				
Likelihood	**Very low (1)**	**Low (2)**	**Medium (3)**	**High (4)**	**Very high (5)**
Very low (1)	Low1	Low 2	Low 3	Medium	Medium
Low (2)	Low	Medium	Medium	Medium	High
Medium (3)	Low	Medium	High	High	High
High (4)	Medium	Medium	High	High	Very High
Very high (5)	Medium	High	High	Very High	Very High

Table 7: Risk evaluation matrix

7.4 NHS Scotland risk appetite statement

7.4.1 NHS Scotland risk appetite is broadly defined as “cautious”: Preference for safe delivery options that have a low degree of residual risk and may only have limited potential for reward. Further guidance on the acceptance of risk is defined based on residual risk values:

Residual risk value	1-3	4-8	9-19	20+
	Risk acceptable	Risk may be acceptable if all methods for further mitigating or avoiding the risk have been considered	Further reduction of risk strongly recommended	Risk unacceptable

Table 8: Residual risk statement options

7.4.2