NHSMAIL O365 SHARED TENANT CLINICAL HAZARD LOG

V4.82

Hazard Summary

CLICK FOR NHSMAIL SUPPORT PAGES

HAZARD	IRR	RRR	PAGE
H1: Adverse system performance impacting communication and workflow	2 - Low	2 - Low	3
H2: Disrupted communication and workflow due to NHSMail outage	3 - Medium	2 - Low	7
H3: Inability to conduct virtual consulations or remote meetings	3 - Medium	2 - Low	13
H4: Inability to send or receive emails and attachments	3 - Medium	2 - Low	16
H5: Breach or loss of confidential patient data during storage and transmission	2 - Low	2 - Low	22
H6: Unable to access encrypted content	3 - Medium	2 - Low	43
H7: Unable to access NHSMail account	3 - Medium	2 - Low	45
H8: Unable to access shared mailbox	2 - Low	2 - Low	56
H9: Guest and external users unable to access shared resources	3 - Medium	2 - Low	58
H10: Unable to administer user accounts	3 - Medium	2 - Low	60
H11: User does not routinely monitor their user/shared mailbox	3 - Medium	2 - Low	62
H12: Updating patient care records; user fails to update the patient care record or updates it with delay	3 - Medium	2 - Low	64
H13: Legitimate emails and attachments are quarantined and/or deleted (false positive)	3 - Medium	2 - Low	65
H14: NHS directory contains incorrect, missing, or duplicate entries	2 - Low	2 - Low	71
H15: User does not maintain their calendar	2 - Low	2 - Low	76
H16: User data fails to fully migrate	2 - Low	2 - Low	80
H17: Accessing third-party (federated) applications	2 - Low	2 - Low	84
H18: The appointment scheduler is unavailable or inaccessible	3 - Medium	2 - Low	86
H19: Patient does not receive appointment invite	3 - Medium	2 - Low	90
H20: User cannot access Microsoft O365 applications or features	3 - Medium	2 - Low	94

IMPORTANT!

The Residual Risk Rating indicated in the table has been derived on the assumption that the controls and mitigations assigned to the 'Local Organisation' will be implemented. If this is not done, the RRR will be higher than stated.

HAZARD ASSESSMENT CRITERIA

Likelihood						
	Very High	3	4	4	5	5
	High	2	3	3	4	5
	Medium	2	2	3	3	4
	Low	1	2	2	3	4
	Very Low	1	1	2	2	3
		Minor	Significant	Considerable	Major	Catastrophic
		Severity				

Likelihood Category	Interpretation
Very high	Certain or almost certain; highly likely to occur
High	Not certain but very possible; reasonably expected to occur in the majority of
Medium	Possible
Low	Could occur but in the great majority of occasions will not
Very low	Negligible or nearly negligible possibility of occurring

5	Unacceptable level of risk
4	Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level
3	Undesirable level of risk. Attempts should be made to eliminate the hazard or implement control measures to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical
2	Acceptable where cost of further reduction outweighs benefits gained or where further risk reduction is impractical
1	Acceptable, no further action required

Severity Classification	Interpretation	Number of Patients Affected
Catastrophic	Death	Multiple
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Multiple
Major	Death	Single
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Single
	Severe injury or severe incapacity from which recovery is expected in the short term	Multiple
	Severe psychological trauma	Multiple
Considerable	Severe injury or severe incapacity from which recovery is expected in the short	Single
	Severe psychological trauma	Single
	Minor injury or injuries from which recovery is not expected in the short term	Multiple
	Significant psychological trauma	Multiple
Significant	Minor injury or injuries from which recovery is not expected in the short term	Single
	Significant psychological trauma	Single
	Minor injury from which recovery is expected in the short term	Multiple
	Minor psychological upset; inconvenience	Multiple
Minor	Minor injury from which recovery is expected in the short term; minor psychological upset; inconvenience; any negligible consequence	Single

HAZARD ID: H1 HAZARD: Adverse system performance impacting communication and workflow

V4.82

Hazard Event: The top event is a sustained period of poor network performance, resulting in a reduced quality of service for NHSMail and associated Office 365 services.

Key Hazard Assumptions 1.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.

Linked Hazards: H2: Disrupted communication and workflow due to NHSmail outage

Context: The NHSmail O365 Shared Tenant aims to provide seamless performance to over 1.4m users. The service must respond instantly to sudden fluctuations in user demand and accommodate the concurrent use of a wide range of O365 applications.

Hazard Event: The top event is a sustained period of poor network performance, resulting in a reduced quality of service for NHSMail and associated Office 365 services.

Cause/s: See possible caues below

Effect: The performance of NHSMail and other related Office 365 services becomes significantly degraded. Users may experience slow email transmission, delays in loading documents or accessing cloud storage, and difficulties in scheduling or updating appointments.

Harm: Potential patient harm may occur due to delays in receiving critical health information or communication from healthcare providers; incorrect or suboptimal treatment decisions could be made due to delays in accessing necessary patient data; rescheduling or managing appointments might be difficult, leading to potential missed treatments or prolonged waiting times; and patients may experience stress and anxiety due to communication delays or miscommunication.

Service/s: Email Gateway (Relay); Microsoft Office 365 Online (SaaS)

Application/s: Exchange Online; Outlook On The Web; Teams; SharePoint; OneDrive

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS); Amazon Web Services (IaaS)

Category: Performance

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Low **Initial Clinical Risk:** 2 - Low

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
275	Technical - Email Gateway: Failure of critical email gateway infrastructure component, e.g. network traffic, CPU utilisation, DNS, suboptimal security scanning configuration etc.	v4.72.4	808	Existing Control: Business Process Change - Changes (including emergency/non-routine and configuration) are logged, authorised, tested, approved and documented before release into the Production environment.	Amazon	AWS System and organisation Controls Report	v4.65.2
			803	Existing Control: Business Process Change - AWS CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing a unified view of AWS resources, applications and services that run on AWS, and on-premises servers. This information is reviewed by the NHSmail Service Management team and used in capacity planning and event monitoring.	Accenture	Amazon CloudWatch	v4.65.2
			306	Existing Control: Design - The Email Gateway uses load balancing and autoscaling to handle tens of millions of requests per second and maintain high throughput and ultra-low latency. As load is increased within the gateway environment, new instances will automatically be provisioned to service increases in processing demand.	Amazon	Elastic Load Balancing and Amazon EC2 Auto Scaling	v4.65.2

Hazard Event: The top event is a sustained period of poor network performance, resulting in a reduced quality of service for NHSMail and associated Office 365 services.

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
275	Technical - Email Gateway: Failure of critical email gateway infrastructure component, e.g. network traffic, CPU utilisation, DNS, suboptimal security scanning configuration etc.	**v4.72.4**	805	Existing Control: Business Process Change - AWS Service Health and Personal Health Dashboards communicate alerts and remediation guidance for managing adverse events. Accenture also subscribes to the AWS Premium Support service, providing direct access to the AWS customer support team and proactive alerts for NHSmail service issues. Performance issues will be communicated on the NHSmail Support site.	Accenture	Announcements	v4.65.2
			806	Existing Control: Business Process Change - AWS details commitments made regarding delivery or performance of services. These details are published in the Service Level Agreements (SLAs) available for each in-scope service. The Email Gateway Service Level Agreement (SLA) for message delivery is 95% delivered within 3 minutes or less. External gateway to email service mailbox is 95% delivered within 3 minutes or less.	Amazon	Service Level Performance Summary	v4.65.2
			804	Existing Control: Business Process Change - AWS maintains a capacity planning model to assess infrastructure usage and demands and to forecast future capacity requirements. The NHSmail Capacity Plan inputs into this.	Amazon	AWS System and organisation Controls Reports	v4.65.2
343	Human Factor - Security filters configuration: Changes to the email gateway security filters, e.g. anti-spam pattern file update, may result in latency issues if the configuration is incorrect, e.g. unsupported character/string.	**v4.72.5**	1035	Additional Control: Testing - Testing is done on all changes to the security filters before release into the Production environment. Regression test packs include the findings of previous incidents to minimise the risk of their reoccurrence.	Trend Micro		v4.73
			1036	Existing Control: Business Process Change - Network alarming will automatically notify service management where mail delivery queues exceed typical thresholds.	Accenture		v4.73
			1037	Existing Mitigation: Business Process Change - Service Management can invoke roll-back procedures to revert to the previous stable release.	Trend Micro		v4.73

Application/Service Exchange Online; Outlook On The Web; Portal; Egress Gateway

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
238	Technical - Azure subservice infrastructure performance: Microsoft Azure and MS Data Centre subservice infrastructure used to host and run the Exchange Online and Egress encryption gateway services e.g. CPU resource exceeded, network configuration, hardware failure.	**v4.63.2**	4	Additional Control: Business Process Change - Capacity metrics measure and monitor network utilisation across all subsystems, from servers to network, and respond to increases and periodic spikes and surges in network traffic. Accenture work with NHSE and Microsoft to plan capacity requirements in line with the NHSmail roadmap and projected user volumes.	Accenture		v1.0

Hazard Event: The top event is a sustained period of poor network performance, resulting in a reduced quality of service for NHSMail and associated Office 365 services.

Application/Service Exchange Online; Outlook On The Web; Portal; Egress Gateway

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
238	Technical - Azure subservice infrastructure performance: Microsoft Azure and MS Data Centre subservice infrastructure used to host and run the Exchange Online and Egress encryption gateway services e.g. CPU resource exceeded, network configuration, hardware failure.	**v4.63.2**	651	Existing Control: Business Process Change - Local organisations have a service desk function enabling end-users to report usability/performance issues. If the local service desk cannot provide a resolution, a service incident can be raised with the NHSmail help desk.	Local Organisation	Contact NHSmail Service Desk	v4.63
			523	Additional Control: Business Process Change - Alerts have been configured against service operations and performance metrics, e.g. CPU utilisation reaches 80%. The automated alerting workflow will notify the appropriate on-call engineers as incidents are created and dealt with based on their priority level.	Microsoft	Azure Monitor	v4.61
			792	Existing Control: Business Process Change - Azure details commitments made regarding delivery or performance of services. These details are published in the Service Level Agreements (SLAs) available for each in-scope service. Compliance monitoring is reported each month against the NHSmail O365 Shared Tenant SLA requirements.	Microsoft	Service-level agreements	v4.65.2
			465	Existing Control: Design - Email systems listed on the DCB1596 accredited secure email allow list will bypass the Egress Gateway encryption service, reducing the processing time and performance demands on the gateway network.	Trend Micro	DCB1596: Secure Email Standard	v4.61
			898	Existing Control: Business Process Change - The NHSMail Portal help pages provide Local Administrators with advisory notices of any performance issues affecting the O365 Online service.	Accenture	Announcements	v4.65.2
			797	Existing Control: Business Process Change - Microsoft notifies customers of potential changes, events and incidents that may impact availability through an online Service Dashboard. The online Service Dashboard is updated in real-time, and RSS feeds are also available for subscription.	Microsoft	Announcements	v4.65.2
			796	Existing Control: Business Process Change - All changes are reviewed and tested, at a minimum, for their quality, performance, impact on other systems, recovery objectives and security features before they are moved into production using a defined release process.	Microsoft	Microsoft System and organisation Controls Reports	v4.65.2

Hazard Event: The top event is a sustained period of poor network performance, resulting in a reduced quality of service for NHSMail and associated Office 365 services.

Application/Service Health and Social Care Network; Internet

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
289	Technical - Local network bandwidth: Local organisation network bandwidth insufficient to meet needs to service.	**v4.65.2**	857	Additional Control: Design - Exchange Online uses Cached Exchange Mode to save a local copy of the mailbox to the users computer. Once email messages have been pulled over the network, subsequent access to those messages does not cause additional network traffic/load.	Microsoft	Cached Exchange Mode	v4.65.3
			471	Existing Control: Design - Egress Large File Transfer functionality, which can send encrypted files up to 5 GB, uses an Egress secure cloud file store to upload and download local content, minimising any performance impact on the local network.	Egress	Egress large file transfer web form	v4.61
			3	Additional Control: Training - Local organisations can have a Microsoft Network Performance Assessment before onboarding to O365 Online to ensure that they have sufficient network capacity to run the O365 applications [this is not a part of standard service offering].	Local Organisation	Preparing for Teams – Technical Guidance for Local Administrators	v4.63
			824	Existing Control: Business Process Change - Local organisations should work with their Consumer Network Service Provider (CNSP) to ensure provision of a network and infrastructure capable of supporting systems needed to run the NHSmail and the O365 services/applications.	Local Organisation		v4.65.3
290	Technical - HSCN Bandwidth: HSCN WAN service network bandwidth insufficient to meet needs to service.	**v4.65.2**	852	Existing Control: Business Process Change - HSCN CN-SP providers must adhere to the HSCN Obligations Framework for the supply, delivery and operation of HSCN Connectivity Services to HSCN Consumers. This includes the reporting of CNSP WAN performance service levels measuring key performance metrics - latency, jitter, packet loss.	NHS England	HSCN Obligations Framework	v4.65.3
			853	Additional Control: Design - The HSCN network implements a Quality of Service configuration to prioritise key network traffic during periods of congestion.	NHS England	HSCN Quality of Service (QoS) Policy	v4.65.3

HAZARD ID: H2 HAZARD: Disrupted communication and workflow due to NHSMail outage

V4.82

Hazard Event: The top event is a prolonged loss of connectivity to Office 365 services, affecting thousands of users simultaneously and persisting for several hours.

Key Hazard Assumptions None Recorded

Linked Hazards: H1: Adverse system performance impacting communication and workflow

Context: The NHSmail O365 Shared Tenant is hosted in a multi-cloud environment. The O365 (SaaS) applications share many of the same infrastructure components. Failure of one or more critical infrastructure components may result in the unavailability of one or more core applications/services, including Teams, Exchange Online and the Email Gateway.

Hazard Event: The top event is a prolonged loss of connectivity to Office 365 services, affecting thousands of users simultaneously and persisting for several hours.

Cause/s: See possible caues below

Effect: NHSMail users, including healthcare professionals, administrators, and other support staff, are unable to access essential email services, calendar scheduling, and cloud storage. This immediately impacts the ability to send, receive, and view emails, access patient records, schedule appointments, and share important documents.

Harm: The primary harm is a significant delay in patient care, as healthcare providers lose a crucial communication tool, and many scheduled virtual appointments are missed. This also leads to a breakdown in communication between healthcare teams, leading to potential errors and oversights. There may also be increased workload and stress for IT teams trying to resolve the issue, and subsequent recovery and backlog management efforts once the system is restored.

Service/s: Amazon Web Services (IaaS); Azure (IaaS); Microsoft Datacentres (IaaS)

Application/s: Microsoft Office 365 Online (SaaS)

Subservice/s:

Category: Availability

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** High **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Amazon Web Services (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
8	Technical - Unplanned downtime: Unavailability of one of more Amazon hosting infrastructure components resulting in service unavailability, e.g. WAN failure, DNS outage, DC outage, AD server failure , Cyber attack, unauthorised change.	v4.65.6	919	Existing Control: Business Process Change - AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.	Amazon	AWS Controls	v4.65.3
			915	Existing Control: Design - Databases are backed up in multiple physical locations as part of normal operation of those services. Services such as Amazon S3, use enhance object durability by protecting data across multiple availability zones on the initial write and then actively doing further replication in the event of device unavailability or detected data loss.	Amazon	AWS Controls	v4.65.3
			916	Existing Control: Business Process Change - Service Management - AWS CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing a unified view of AWS resources, applications and services that run on AWS, and on-premises servers. This information is reviewed by the NHSmail Service Management team and used in capacity planning and event monitoring.	Accenture	AWS Controls	v4.65.3

Hazard Event: The top event is a prolonged loss of connectivity to Office 365 services, affecting thousands of users simultaneously and persisting for several hours.

Application/Service Amazon Web Services (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
8	Technical - Unplanned downtime: Unavailability of one of more Amazon hosting infrastructure components resulting in service unavailability, e.g. WAN failure, DNS outage, DC outage, AD server failure , Cyber attack, unauthorised change.	v4.65.6	917	Existing Control: Business Process Change - Changes are implemented in a phased deployment and closely monitored for any impact. Baseline metrics are used to measure the health of the services upstream, and metrics are closely monitored with thresholds and alarming in place (e.g., latency, availability, fatals, CPU utilisation, etc.).	Amazon	AWS Controls	v4.65.3
			548	Additional Control: Testing - Business Continuity and Disaster Recovery testing are undertaken once a year to assure the completeness, accuracy, workability and reliability of the BCDR plan and failover processes. NHS England are invited to witness this.	Accenture	Testing disaster recovery	v4.65.1
			914	Existing Control: Design - Data centres are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+ 1 standard, so that in the event of a data centre failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.	Amazon	AWS Controls	v4.65.3
			547	Additional Control: Business Process Change - The local organisation will assume responsibility for local service availability issues (e.g. local network or other systems outside NHSmail). Local organisation Business Continuity and Disaster Recovery plans will serve as controls.	Local Organisation	Business continuity	v4.65.1
			913	Existing Control: Business Process Change - AWS applies a systematic approach to managing change so that changes to customer impacting services are reviewed, tested, approved, and well communicated. Change management processes are based on Amazon change management guidelines and tailored to the specifics of each AWS service.	Amazon	AWS Controls	v4.65.3
			154	Additional Control: Testing - Organisations should undertake local risk assessments and testing of new IP addresses to ensure that they can resolve DNS requests against any new IP address configuration.	Local Organisation	Relay Configuration	v4.61
			545	Existing Control: Business Process Change - Service Management provides 24x7 Level 3 support for critical business issues. Incidents that involve the AWS infrastructure are escalated to the L3 Accenture support team within Service Now, and the on-call rota is utilised for any HSSI. AWS Cloud watch is utilised to monitor and alert proactively to the corresponding teams and incidents raised once an alert is validated. These are then managed through the standard incident management process. If the incident is deemed to be a fault with AWS availability zones or infrastructure, then a case is raised with AWS support from the console on the account where the infrastructure sits.	Accenture		v4.65.1

Hazard Event: The top event is a prolonged loss of connectivity to Office 365 services, affecting thousands of users simultaneously and persisting for several hours.

Application/Service Amazon Web Services (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
8	Technical - Unplanned downtime: Unavailability of one of more Amazon hosting infrastructure components resulting in service unavailability, e.g. WAN failure, DNS outage, DC outage, AD server failure , Cyber attack, unauthorised change.	v4.65.6	944	Existing Control: Design - WAN connectivity between the on-premise datacentres and AWS data centres is provided through AWS Direct Connect circuit using Cloud Link connections as a resilient pair.	Amazon	AWS Direct Connect	v4.65.6

Application/Service Egress Email Gateway

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
151	Business Process - Service Maintenance: Egress is permitted 24hrs of planned downtime per calendar month to undertake essential maintenance.	v4.61	448	Existing Control: Business Process Change - Planned downtime will only be undertaken during off-peak hours when the impact to live service is least likely to impact end-users.	Accenture		v4.63.2
			310	Existing Control: Design - The Egress service employs a resilient architecture designed to ensure service continuity when components, such as servers and interfaces, are temporarily out of action due to scheduled maintenance.	Egress	Egress Hosting Infrastructure	v4.61
			311	Additional Control: Business Process Change - Egress will notify NHS England 4 weeks in advance of any planned maintenance. Planned maintenance is also communicated on the Egress Web Portal.	Egress	Egress Service Status	v4.61
			312	Additional Control: Business Process Change - NHS England will issue communications to Local Administrators when maintenance is planned and make this known on the NHSmail Announcements page.	NHS England	Announcements	v4.61

Application/Service Microsoft Azure (IaaS); Microsoft Datacentres (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
4	Technical - Unplanned downtime: Unavailability of one of more Microsoft hosting infrastructure components resulting in service unavailability, e.g. WAN failure, DC outage, AD server failure, Cyber attack.	v4.61	529	Existing Control: Business Process Change - The NHSmail Portal provides live information on the service status of the NHSmail services. Local Administrators can also subscribe to the NHSmail High Severity Service Incident (HSSI) alerting service, which will provide ongoing status updates until the incident is resolved.	Accenture	Service Status	v4.61

Hazard Event: The top event is a prolonged loss of connectivity to Office 365 services, affecting thousands of users simultaneously and persisting for several hours.

Application/Service Microsoft Azure (IaaS); Microsoft Datacentres (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
4	Technical - Unplanned downtime: Unavailability of one of more Microsoft hosting infrastructure components resulting in service unavailability, e.g. WAN failure, DC outage, AD server failure, Cyber attack.	v4.61	748	Additional Control: Business Process Change - Where a change has been implemented by Accenture resulting in the unavailability of the service, rollback procedures can be invoked by Service Management to restore access. N.B. Accenture may implement a fix forward stance but data replication ensures that all data is backed up and service restoration will adhere to SLA timescales.	Accenture		v4.65.2
			716	Existing Control: Design - Proactive monitoring continuously measures the performance of critical subsystems of the Office 365 services platform against the established boundaries for acceptable service performance and availability. When a threshold is reached or a rare event occurs, the monitoring system generates warnings so that operations staff can address the threshold or event.	Microsoft	Azure Monitor	v4.63.2
			403	Existing Control: Design - Customer data is automatically replicated within Azure to minimise isolated faults and critical components have been designed with redundancy to sustain isolated faults and minimise disruption to services.	Microsoft	Azure Storage redundancy	v4.65.2
			612	Additional Control: Testing - Microsoft's Enterprise Business Continuity Management (EBCM) policy stipulates that all Microsoft business continuity and disaster recovery plans must be tested, updated, and reviewed annually. Failover exercises are frequently undertaken to test applications and related data to verify the accessibility at a secondary disaster recovery location, in line with the recovery time objective (RTO).	Microsoft	Resiliency and continuity overview	v4.63.2
			858	Additional Control: Design - Exchange Online uses Cached Exchange Mode to save a local copy of the mailbox to the users computer, enabling email access when in offline mode.	Microsoft	Cached Exchange Mode	v4.65.2
			856	Additional Control: Design - Exchange ActiveSync enables users of mobile devices to continue to access their email, calendar, contacts, and tasks during periods of network outage.	Microsoft	Exchange ActiveSync	v4.65.2
			945	Existing Control: Design - WAN connectivity between the on-premise data centres and Azure data centres is provided through Azure ExpressRoute using Cloud Link connections as a resilient pair.	Microsoft	Azure ExpressRoute	v4.65.6

Hazard Event: The top event is a prolonged loss of connectivity to Office 365 services, affecting thousands of users simultaneously and persisting for several hours.

Application/Service Microsoft Azure (IaaS); Microsoft Datacentres (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
4	Technical - Unplanned downtime: Unavailability of one of more Microsoft hosting infrastructure components resulting in service unavailability, e.g. WAN failure, DC outage, AD server failure, Cyber attack.	**v4.61**	7	Existing Control: Business Process Change - Microsoft service engineers are on call 24x7 to monitor and resolve issues that are reported or identified. Each service utilises customer tools to monitor capacity, resiliency and availability to identify anomalies or deviations that could impact availability. The service operates an SLA backed Recovery Point Objective (RPO) of 5 minutes and the Recovery Time Objective (RTO) of 4 hours.	Microsoft	Microsoft System and organisation Controls Reports	v4.63
			802	Existing Control: Business Process Change - Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements. The availability of Azure services is monitored through third-party and internal tools, and the status is communicated through a Service Dashboard. The errors generated during the job execution are monitored and appropriate action is taken based on the job settings defined by the customer administrator.	Microsoft	Enterprise-scale business continuity and disaster recovery	v4.65.2

Application/Service Microsoft Azure (IaaS); Microsoft Datacentres (IaaS); Amazon Web Services (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
6	Business Process - Planned downtime: Unavailability due to essential maintenance or transition activities.	**v4.63**	774	Existing Control: Business Process Change - Changes involving planned downtime are done during periods of low user activity to minimise any impact on end-users. All changes are required to pass testing in an environment that replicates Production as closely as possible. Testing will also include rollback procedures should the change fail. Third party suppliers undertake testing in accordance with their own procedures and failure of those changes is managed via SLAs.	Accenture		v4.65.1
			918	Existing Control: Business Process Change - Maintenance is usually undertaken as a live update to minimise end-user impact. If a live update is not possible, a scheduled maintenance event is required, and this will be communicated on the NHSmail Portal.	Accenture	Announcements	v4.65.3
			411	Existing Control: Business Process Change - Changes that can impact end-users will be communicated to Local Administrators in advance, using multiple channels, such as direct comms, LA Bulletin and weekly webinar. Significant changes will also be posted on the NHSMail Portal help pages.	NHS England	Announcements	v4.61
			446	Existing Control: Business Process Change - Office365 has developed formal standard-operating-procedures (SOPs) governing the change-management process. SOPs cover both software development and hardware change and release management, and are consistent with established regulatory guidelines including ISO 27001, SOC 1/SOC 2, NIST 800-53, and others.	Microsoft	Service organisation Controls (SOC)	v4.63.2

HAZARD ID: H2 HAZARD: Disrupted communication and workflow due to NHSMail outage V4.82

Hazard Event: The top event is a prolonged loss of connectivity to Office 365 services, affecting thousands of users simultaneously and persisting for several hours.

Application/Service Microsoft Azure (IaaS); Microsoft Datacentres (IaaS); Amazon Web Services (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
6	Business Process - Planned downtime: Unavailability due to essential maintenance or transition activities.	v4.63	776	Additional Control: Design - If the Portal is unavailable due to planned maintenance, a message/page will inform the end-user.	Accenture		v4.65.5
			777	Existing Control: Design - If the Portal is unavailable due to planned maintenance, users can still access their email account via Outlook on the Web (email.nhs.net) and the O365 applications.	Local Organisation		v4.65.1

HAZARD ID: H3 HAZARD: Inability to conduct virtual consulations or remote meetings

V4.82

Hazard Event: The top event is a prolonged period of inaccessibility to Teams A&VC or Phone System, impeding real-time communication for healthcare providers and patients.

Key Hazard Assumptions 1.The user can login to their account.2.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.3. The O365 Teams application can be accessed.

Linked Hazards: H2: Disrupted communication and workflow due to NHSmail outage; H7: Unable to access NHSmail account; H20: Accessing Microsoft applications and features

Context: Microsoft Teams provides audio and video conferencing (A&VC) and outbound calling via the Teams Phone System. A&VC can be used to host patient consultations as part of the Virtual Visits service (subject to local set-up), or it can be used standalone. The Teams Phone system can increase capacity by freeing up existing phone lines for incoming calls, e.g. at GP practices during peak times. Teams also can be used to communicate with Guest/External users (subject to local set-up). *Important! the Teams Phone System is not advised for emergency calling*

Hazard Event: The top event is a prolonged period of inaccessibility to Teams A&VC or Phone System, impeding real-time communication for healthcare providers and patients.

Cause/s: See possible caues below

Effect: Users are unable to conduct or participate in audio or video meetings, and cannot use the phone system. This impacts communication, collaboration, and decision-making processes, particularly in healthcare settings where real-time communication is crucial.

Harm: The potential harm to patients could include delays in diagnosis or treatment due to the inability to conduct virtual consultations; potential for errors due to miscommunication or inability to communicate promptly; missed appointments due to lack of reminder calls or rescheduling; patient distress or anxiety due to poor communication or lack of contact with healthcare providers.

Service/s: Microsoft Office 365 Online (SaaS) **Application/s:** Teams **Subservice/s:** Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Access **Hazard Status:** Open **Status Comment:** **Hazard Updated:** v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Microsoft Teams

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
107	Technical - Meeting link error: The Teams 'join meeting link' or 'Join Meeting' button does not allow the user to access the consulation.	V4.64.2	727	Additional Control: Testing - Testing will be performed to validate staff members can consult with patients (joining in as guests).	Accenture	Private beta testing (internal document)	v4.64.2
			729	Additional Control: Training - Guidance is provided on how to join a Teams meetings.	NHS England	How to join a Microsoft Teams meeting	v4.65.5
248	Human Factor - Teams accessibility: End-user is unable to operate the A&VC software, preventing them from accessing or continuing with the consultation, e.g. may be unable to activate the camera or microphone or have accessibility needs, e.g. hearing impairment.	V4.64.2	753	Additional Control: Design - The Teams application has several accessibility settings, such as live captions, zoom, dark/light mode and immersive reader.	Microsoft	Accessibility Settings in Teams	v4.64.2
			755	Additional Control: Training - Guidance is provided on how to activate the Teams Accessibility settings.	NHS England	Accessibility Settings in Teams	v4.64.2

HAZARD ID: H3 HAZARD: Inability to conduct virtual consulations or remote meetings

Hazard Event: The top event is a prolonged period of inaccessibility to Teams A&VC or Phone System, impeding real-time communication for healthcare providers and patients.

Application/Service Microsoft Teams

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
248	Human Factor - Teams accessibility: End-user is unable to operate the A&VC software, preventing them from accessing or continuing with the consultation, e.g. may be unable to activate the camera or microphone or have accessibility needs, e.g. hearing impairment.	**V4.64.2**	238	Additional Control: Business Process Change - It the patient is experiencing usability issues that are so significant that the video consultation cannot safely continue, an alternative communication channel can be used, e.g. revert to a phone call or offer a face-to-face appointment.	Local Organisation	Virtual Consultation (FAQ)	v4.63
			386	Additional Control: Training - Guidance is provided on the use of the Teams app, including how to customise the settings and activate the webcam and microphone.	NHS England	Virtual Consultation	v4.63
249	Technical - System requirements: The A&VC software is unavailable for download or the patient is unable to install it on their device, e.g. phone setting policies or software version may limit what apps can be installed.	**V4.63**	385	Existing Control: Business Process Change - Patients who cannot or do not wish to download the mobile or desktop app can access the consultation through the web browser.	Local Organisation	Use Teams on the web	v4.65.5
			712	Existing Control: Testing - Access to Teams has been successfully tested using various web browsers and operating systems (Google Chrome, Edge, Explorer 11, Safari, Android).	Accenture		v4.65.5
251	Human Factor - Teams configuration: Users may be unable to access the Teams application if the Local Administrator has not completed the required technical pre-requisites within the Portal, e.g. opening of ports/setting of IP address ranges.	**V4.64.2**	754	Additional Control: Training - Guidance is provided on the technical pre-requisites required to access Teams performance, e.g., firewall ports, inbound protocols, endpoints, IP addresses, and URLs	NHS England	Preparing for Teams – Technical Guidance for Local Administrators	v4.64.2

Application/Service Networks

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
9	Technical - Bandwidth: Insufficient network bandwidth results in unacceptable interference (jitter, hang or freeze) or the sudden termination of the call.	**V4.61**	617	Additional Control: Business Process Change - Microsoft provides a Teams network bandwidth calculator that enables local organisations to enter information about the planned user numbers and server features to be deployed. The calculator will determine the bandwidth requirements needed for a stable network connection.	Local Organisation	Microsoft Teams admin documentation	v4.63
			616	Existing Control: Design - Teams is designed to manage expected spikes in traffic and increased usage over time. A&VC endpoints can adapt to varying network conditions and support three times the throughput whilst still maintaining acceptable quality.	Microsoft		v4.63

Hazard Event: The top event is a prolonged period of inaccessibility to Teams A&VC or Phone System, impeding real-time communication for healthcare providers and patients.

Application/Service Networks

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
9	Technical - Bandwidth: Insufficient network bandwidth results in unacceptable interference (jitter, hang or freeze) or the sudden termination of the call.	**V4.61**	611	Additional Control: Design - Local organisations with network bandwidth restrictions can use a Quality of Service (QoS) configuration to prioritise network traffic for audio/video/desktop sharing. This configuration will reduce the risk of users encountering latency, jitter and drop-out.	Local Organisation	Implement Quality of Service (QoS) in Microsoft Teams	v4.63
			693	Additional Control: Business Process Change - If Teams A&VC cannot be used and the meeting cannot be rescheduled, PSTN dial-in, or an alternative network connection, can be used. (NHSX has approved the use of encrypted services WhatsApp and Facetime where no other alternative A&VC service is available during the COVID-19 period).	Local Organisation	COVID-19 IG advice	v4.63
			556	Additional Control: Training - Guidance is provided on the minimum bandwidth requirements for A&VC peer to peer and group calling.	NHS England	Preparing for Teams – Technical Guidance for Local Administrators	v4.64

Application/Service Teams Phone System (Outbound Calling)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
322	Business Process - Phone system licence allocation: The Phone System and Calling Plan licences have not been applied to the User Policy or have been removed in error.	**v4.66.1**	954	Additional Control: Design - The Local Administrator can reallocate the Phone System and Calling Plan licences in User Policy Management.	Local Organisation	User Policy Management	v4.67.1
			953	Additional Control: Design - The Microsoft 365 Phone System and Calling Plan licences will be bulk assigned to eligible users.	Accenture	Teams Phone System for Outbound Calls	v4.67.1
324	Technical - Calling plan minutes : The service call plan has a limited number of call minutes, and all GP practices on the Tenant must share these. When the minutes have been used, it is not possible to make outbound calls.	**v4.66.1**	955	Existing Control: Business Process Change - The GP practice can revert to analogue PSTN or mobile network.	Local Organisation		v4.66.1

HAZARD ID: H4 HAZARD: Inability to send or receive emails and attachments

V4.82

Hazard Event: The top event is a prolonged disruption in the ability to send or receive emails and attachments, despite the availability of infrastructure.

Key Hazard Assumptions 1.The user can login to their account.2.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.3. The O365 Exchange Online/Web application can be accessed.

Linked Hazards: H2:Disrupted communication and workflow due to NHSMail outage; H7:Unable to access NHSMail account; H20:User cannot access Microsoft O365 applications or features

Context: Care information is sent in the email and commonly as a file attachment. Even in the absence of NHSmail O365 Shared Tenant outage or login issues, email delivery and receipt can be affected by local set-up issues, Exchange Online quota limits or external factors, such as HSCN network unavailability.

Hazard Event: The top event is a prolonged disruption in the ability to send or receive emails and attachments, despite the availability of infrastructure.

Cause/s: See possible caues below

Effect: Users can't send or receive emails or attachments, significantly impacting communication and the sharing of important documents, even though the overall system infrastructure is available and functioning.

Harm: Patient harm could potentially occur in several ways: important health information might not be communicated in a timely manner; treatment instructions or prescription details could be delayed; appointment updates or scheduling information could be missed; patients might not receive timely responses to their queries, causing stress or anxiety; crucial documents such as medical reports or consent forms might not be shared or received.

Service/s: Microsoft Office 365 Online (SaaS) **Application/s:** Exchange Online; Outlook On The Web **Subservice/s:** Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Availability **Hazard Status:** Open **Status Comment:** **Hazard Updated:** v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
13	Technical - File size limit reached: Email messages exceeds limit of 35MB permitted for the NHSmail service or file type is unsupported.	v4.61	104	Additional Control: Training - Guidance is provided on file size and type restrictions.	NHS England	Attachments Guide for NHSmail	v4.61
			21	Existing Control: Design - MailTips functionality in the Outlook Web App (OWA) and Modern Outlook Clients will warn the end-user when the email size limit has been exceeded. Reducing the size will enable the email to be sent.	Microsoft	MailTips	v4.63
			325	Existing Control: Business Process Change - Egress Switch Large File Transfer (LFT) enables files of up to 5GB to be uploaded to a secure Egress Cloud storage area, which has no impact on the end-users email quota.	Local Organisation	Egress large file transfer web form	v4.61
			289	Existing Control: Business Process Change - Large attachments can be securely shared using the OneDrive or SharePoint external file sharing function.	Local Organisation	Share OneDrive files and folders	v4.65.2
14	Human Factor - File type: End-user attaches an incorrect file type to the email, file transfer or Egress Large File Transfer functionality.	v4.61	291	Additional Control: Training - Guidance is provided on file size and type restrictions.	NHS England	Attachments Guide for NHSmail	v4.61

Hazard Event: The top event is a prolonged disruption in the ability to send or receive emails and attachments, despite the availability of infrastructure.

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
67	Human Factor - Email protocols: Incorrect configuration of the IMAP, POP or SMTP settings by the Local Administrator may prevent emails from being sent and/or received.	v4.65.2	132	Additional Control: Training - Guidance is provided on the configuration of IMAP / POP settings.	NHS England	Enabling and disabling POP IMAP SMTP	v4.65.2
			464	Existing Control: Design - A pop-up window will confirm to the Local Administrator when the email protocol settings have been successfully enabled or disabled.	Accenture	Enabling and disabling POP IMAP SMTP	v4.65.2
			463	Existing Control: Testing - Local changes to the email protocols should be tested to ensure the delivery and receipt of emails functions as intended, e.g. that local firewalls, anti-virus software and ports do not disrupt or block email flow.	Local Organisation	Applications Guide	v4.65.2
			133	Existing Control: Business Process Change - When sending clinical information, e.g. patient referrals, appointments or discharge letters, users have a duty of care to ensure that it is received and acknowledged.	Local Organisation		v4.65.2

Application/Service Exchange Online; Outlook 2010

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
328	Technical - Legacy software: From 1st May 2022, user on MS Outlook 2010 will no longer be able to connect to MS Exchange Online (Outlook 2010, is no longer supported by Microsoft, e.g. security updates are no longer applied). This means that users using NHSmail and Outlook 2010 on a device, will not be able to connect and all emails from Exchange Online will not be delivered and calendars will not sync.	v4.69.2	971	Existing Control: Business Process Change - Local organisations have a responsibility to ensure that they are using software capable of supporting the latest security updates.	Local Organisation		v4.69.2
			972	Existing Control: Business Process Change - Users can continue to access the Outlook Web Application through their browser (portal.nhs.net) or Outlook mobile app.	Local Organisation		v4.69.2
			973	Additional Control: Training - Guidance is provided on the end of life of Office 2010 (including Outlook). This includes direct end-user/LA comms, LA Bulletin and Portal Announcements.	NHS England	Office 2010 important end date reminder	v4.69.2

Hazard Event: The top event is a prolonged disruption in the ability to send or receive emails and attachments, despite the availability of infrastructure.

Application/Service Exchange Online; Outlook 2010

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
328	Technical - Legacy software: From 1st May 2022, user on MS Outlook 2010 will no longer be able to connect to MS Exchange Online (Outlook 2010, is no longer supported by Microsoft, e.g. security updates are no longer applied). This means that users using NHSmail and Outlook 2010 on a device, will not be able to connect and all emails from Exchange Online will not be delivered and calendars will not sync.	**v4.69.2**	977	Existing Control: Business Process Change - In accordance with the Data Security and Protection toolkit (Data Security Standard 8) Local Organisations should ensure that they survey their IT inventory to understand which assets are approaching end of life. All legacy software should be risk assessed, and if appropriate, treated as unmanaged and untrusted.	Local Organisation	Data Security and Protection Toolkit	v4.69.2
			980	Additional Control: Business Process Change - NHS England has identified the organisations using Outlook 2010 and is working with these to transition to a supported Outlook Client.	NHS England		v4.69.2

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
183	Technical - End-user mailbox quota has been reached: When a user reaches the default mailbox quota of 4GB they will no longer be able to send emails and when they reach their quota plus 1GB, they will no longer be able to receive emails.	**v4.65.2**	418	Additional Control: Business Process Change - Email should be managed and stored in line with the local organisation's Records Management Policy and other relevant policies. The terms and conditions of the NHSmail Acceptable Use Policy should be incorporated into local policies and communicated to end-users. Local Administrators should undertake proactive monitoring of user account mailbox quotas as part of their administrative responsibilities.	Local Organisation	Mailbox Management	v4.65.2
			849	Additional Control: Design - Each user is provided with a 100GB personal email archive. Users can also reduce their inbox by deleting any emails that are no longer needed.	Local Organisation	Exchange Online Archiving Guidance and FAQs	v4.65.2
			405	Additional Control: Business Process Change - Organisations can procure larger mailboxes (outside of the standard 10% 50GB mailbox quota) from a Microsoft licence reseller and onboard these to the NHSmail O365 Shared Tenant.	Local Organisation	Onboarding Guide for Local Administrators	v4.65.2
			408	Existing Control: Design - End-users will receive an automated warning email when their mailbox is 400MB from reaching its mailbox quota and when 1GB has exceeded their default quota.	Microsoft	Managing your mailbox quota	v4.65.2
			406	Additional Control: Training - Guidance is provided on mailbox hygiene, specifically what actions a user needs to take to reduce their mailbox quota to an acceptable level.	NHS England	Managing Mailbox Quota	v4.65.2

Hazard Event: The top event is a prolonged disruption in the ability to send or receive emails and attachments, despite the availability of infrastructure.

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
183	Technical - End-user mailbox quota has been reached: When a user reaches the default mailbox quota of 4GB they will no longer be able to send emails and when they reach their quota plus 1GB, they will no longer be able to receive emails.	**v4.65.2**	675	Additional Control: Design - The Local Administrator can use the User Mailbox Usage and User Dumpster Usage reports to proactively target users nearing a breach of their mailbox quota.	Local Organisation	Admin Reports	v4.65.2
			888	Additional Control: Design - A MailTip will notify the sender when the recipient mailbox is full.	Microsoft	MailTips	v4.65.2
			221	Additional Control: Design - Exchange Online provides users with a 4GB mailbox quota as standard. Administrators who have the “Authorisations” role can increase/decrease the mailbox capacity for mailboxes within their organisation, utilising a 10% quota of 50GB mailboxes. For example, a Shared Mailbox (which does not have a 100GB personal archive) needs to be increased.	Accenture	Managing Mailbox Quota	v4.65.2
293	Business Process - Active Sync configuration error: The local organisation Exchange ActiveSync (EAS) protocol legacy settings have not been updated to the new O365 Tenant configuration [EAS lets mobile phone users access their email, calendar, contacts, and tasks, and lets them continue to access this information when they're working offline].	**v4.65.4**	837	Existing Control: Training - Guidance is provided on reconfiguring the legacy EAS protocol settings to EAS for Exchange Online.	NHS England	Preparing your Application account for Exchange Online	v4.65.5
			836	Existing Control: Business Process Change - NHS England has communicated to Local Administrators the change scope, impacts, and actions required to reinstate email availability to end-user mobile devices. Communications include LA Bulletin, LA Webinar and targeted comms.	NHS England	Retirement of legacy hostnames/service URLs	v4.65.5
			835	Existing Control: Design - End-Users unable to access email on their mobile device can use an alternative Outlook Client, e.g. Outlook, Outlook on the web.	Local Organisation	Clients and mobile devices	v4.65.4
294	Technical - Firewall/Web Proxy configuration: Local Organisations may have restrictions on their firewalls or web proxies preventing connectivity to the Exchange Online service.	**v4.65.3**	838	Existing Control: Training - Guidance is provided on the requisite firewall and web proxy settings for connecting to the O365 shared Tenant.	NHS England	NHSmail Firewall and Proxy Server Access	v4.65.2

Hazard Event: The top event is a prolonged disruption in the ability to send or receive emails and attachments, despite the availability of infrastructure.

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
296	Business Process - Intune (Mobile Device Management) Remote Wipe: Email application has been removed from the end-user device.	**v4.65.3**	842	Existing Control: Design - End-Users unable to access email on their mobile device can use an alternative Outlook Client, e.g. Outlook, Outlook on the web.	Local Organisation	Clients and mobile devices	v4.65.3
298	Business Process - NHSmail hostname/URL configuration: The email legacy hostnames/service URLs for sending and receiving email have not been configured to the O365 Online service.	**v4.65.3**	850	Additional Control: Business Process Change - User accounts sending emails using legacy hostnames/URL's have been identified, and Local Administrators contacted directly to ensure any applicable local applications are reconfigured to use the correct hostnames. Continued monitoring of the legacy settings will continue until the changes are implemented to reduce the impacted accounts to as low as possible.	Accenture		v4.65.3
			848	Additional Control: Business Process Change - Changes to the POP/IMAP/SMTP and Legacy/Exchange ActiveSync hostnames have been communicated to Local Administrators via the NHSmail Portal help pages, LA Bulletin and Webinar.	NHS England	Retirement of legacy hostnames/service URLs	v4.65.5
299	Technical - High-Sending email accounts: Exchange Online application account sending limit has been reached. (messages can't be sent from the mailbox until the number of recipients that were sent messages in the past 24 hours drops below the sending limit).	**v4.65.3**	851	Existing Control: Design - If an application has not been identified or subsequently needs to exceed the Microsoft O365 Outlook sending limits, the Local Administrators can change the SMTP hostname in the Portal (to smtp.office365.com).	Local Organisation	High Sending SMTP Solution	v4.65.3
			847	Additional Control: Business Process Change - Accounts that are likely to exceed Exchange Online default sending limit / routinely send higher volumes of email should use the High Sending SMTP protocol (send.nhs.net) which allows higher throughput and avoids the Exchange Online limit.	Local Organisation	Exchange Online limits	v4.65.5
			846	Existing Control: Training - Guidance is provided on the requirements for high-sending email accounts.	NHS England	Preparing your Application account for Exchange Online	v4.65.3
			930	Existing Control: Design - A Non-Delivery Report (NDR) will be delivered to the sending mailbox where Exchange Online sending limits have been exceeded. Local organisations should monitor the mailboxes for NDRs and take appropriate action.	Local Organisation	High Sending SMTP Solution	v4.65.5

Hazard Event: The top event is a prolonged disruption in the ability to send or receive emails and attachments, despite the availability of infrastructure.

Application/Service Health and Social Care Network; Internet

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
300	Technical - Network Outage: HSCN/Internet WAN/LAN outage resulting in loss of connectivity to the NHSmail Gateway.	**v4.65.3**	854	Existing Control: Business Process Change - HSCN CN-SP providers must adhere to the HSCN Obligations Framework for the supply, delivery and operation of HSCN Connectivity Services to HSCN Consumers. This includes the reporting of CNSP WAN availability service levels (minimum 99.95% availability).	NHS England	HSCN Obligations Framework	v4.65.3
			855	Additional Control: Business Process Change - The HSCN authority will carry out operational monitoring on an ongoing basis to ensure that the service(s) are compliant with the requirements of the HSCN Obligations, including but not limited to business continuity plans, business continuity test plans and results, and failover test plans and results.	NHS England	HSCN Governance	v4.65.3
			338	Additional Control: Business Process Change - The local organisation will assume responsibility for local service availability issues (e.g. local network or other systems outside NHSmail). Local organisation Business Continuity and Disaster Recovery plans will serve as controls.	Local Organisation	Business continuity	v4.61

HAZARD ID: H5 HAZARD: Breach or loss of confidential patient data during storage and transmission

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Key Hazard Assumptions 1.The Local Organisation adheres to the legal framework governing the use of personal confidential data, e.g. NHS Act 2006, the Health and Social Care Act 2012, the Data Protection Act, and the Human Rights Act.

Linked Hazards: None Recorded

Context: Many applications used by the service are used to communicate Patient Confidential Data. Because of this, there any many opportunities both at a human and system level for the malicious or unintentional disclosure of sensitive information.

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Cause/s: See possible caues below

Effect: Confidential patient data is compromised, either being lost, stolen, or accessed by unauthorised individuals. This could result in the loss of patient trust, potential legal implications, and even the misuse of sensitive patient data.

Harm: Potential patient harm could include distress or anxiety due to the invasion of privacy, potential identity theft or fraud if personal information is misused, health implications if medical records are tampered with or if the continuity of care is disrupted due to lost data, and mistrust in the healthcare system, leading to reluctance in sharing critical health information in the future.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: Exchange Online; SharePoint; Teams; Outlook On The Web; Stream

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS); Trend Cloud Application Security (SaaS)

Category: Information Governance and Security

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Low **Initial Clinical Risk:** 2 - Low

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Amazon Web Services (IaaS); Azure (IaaS); Microsoft Datacentres (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
291	Technical - Online data hosting: Internal and external data hosting vulnerabilities may result in the disclosure of patient sensitive data, e.g. malware, ransomware, attack vector.	v4.65.2	362	Existing Control: Business Process Change - Microsoft has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.	Microsoft	Azure Security Centre	v4.65.2
			825	Existing Control: Business Process Change - An audit trail is maintained on AWS environment, which will include who or what took which action, what resources were acted upon, when the event occurred, and other details to help analyse and respond identify and respond to unusual activity.	Accenture	AWS CloudTrail	v4.65.2
			826	Existing Control: Design - AWS implements a variety of activities prior to and after service deployment to further reduce risk within the AWS environment. These activities integrate security and compliance requirements during the design and development of each AWS service and then validate that services are operating securely after they are moved into production (launched).	Amazon	AWS Compliance	v4.65.2
			827	Existing Control: Design - AWS security is built on best practice design principles to prevent, detect, respond and remediate against security incidents and ensure that an optimal security posture is maintained at all times.	Amazon	AWS Cloud Security	v4.65.2

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Amazon Web Services (IaaS); Azure (IaaS); Microsoft Datacentres (IaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
291	Technical - Online data hosting: Internal and external data hosting vulnerabilities may result in the disclosure of patient sensitive data, e.g. malware, ransomware, attack vector.	**v4.65.2**	243	Existing Control: Design - NHSmail O365 is being managed as a single-tenant within Microsoft UK and EU data centres; a single-tenant architecture is considered more secure. The hosting environment is continually monitored for malicious activity and audit logs generate alerts for each event. All administrative actions are audited and access is controlled through conditional. All data is encryption in transit and at rest.	Microsoft	Azure Monitor	v4.63

Application/Service Azure AD B2B Direct Connect

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
340	Human Factor - Information Sharing: Unauthorised access to shared resources (Note: disabling a user's access will not take effect until the access token has expired (up to 1 hour).	**v4.80.1**	1021	Existing Control: Design - Sensitivity labels designated for the Team are configured to be automatically applied to Shared Channels.	NHS England		v4.80.1
			1018	Existing Control: Business Process Change - Local Administrators may submit a service desk request for access to Azure AD sign-in logs to validate external user access via B2B Direct Connect and oversee policy modifications.	Local Organisation		v4.80.1
			1020	Existing Control: Training - Comprehensive guidance is provided for both the configuration and utilisation of the B2B Direct Connect service, including the implications of establishing a Shared Channel.	NHS England		v4.80.1
			1022	Existing Control: Design - The B2B Direct Connect service restricts channel membership to users selected by the Teams Shared Channel owner, who holds exclusive authority to add new members.	NHS England		v4.80.1
			1024	Existing Control: Business Process Change - Team Owners or Shared Channel Owners should regularly audit membership lists, revoking access as necessary. The Teams access review feature is available to assist in this process.	Local Organisation		v4.80.1
			1026	Additional Control: Business Process Change - Local organisations must complete a verified onboarding process, providing evidence of compliance with either DCB1596 or ISO 27001 standards, prior to policy activation.	Local Organisation		v4.80.1
			1027	Additional Control: Design - File sharing capabilities are limited exclusively to individuals who hold membership in the shared channel.	Microsoft		v4.80.1

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Azure AD B2B Direct Connect

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
340	Human Factor - Information Sharing: Unauthorised access to shared resources (Note: disabling a user's access will not take effect until the access token has expired (up to 1 hour).	**v4.80.1**	1019	Existing Control: Design - By default, the B2B Direct Connect settings are configured to prohibit access from all external organisations.	NHS England		v4.80.1

Application/Service Azure AD B2B Guest Access

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
123	Human Factor - O365 B2B Guest invites: Guest Inviter may send B2B guest invites to users of an unauthorised external organisations.	**v4.63**	627	Additional Control: Design - External sharing outside of the NHSmail O365 Shared Tenant has been disabled and only guests from organisations added to an approved allow list controlled by the Global Administrator can access shared resources. Invites must come from a user that has been assigned (via RBAC) as a 'guest inviter.'	NHS England	Guest Access Guidance	v4.65.5
			254	Existing Control: Business Process Change - External sharing is only available to users that have been configured as 'Eligible Guest Inviters' by their NHSmail Local Administrator.	Local Organisation	External collaboration using Azure B2B guest access service	v4.65.6
125	Technical - Guest domain compromised: O365 B2B external guest domain has been compromised.	**v4.63**	256	Existing Control: Business Process Change - If a domain becomes compromised, it can be disabled by the NHSmail Live Services Administrator.	NHS England	Create a guest access allow list request	v4.63
126	Human Factor - Information sharing: The administrator does not manage guest access appropriately.	**v4.63**	260	Existing Control: Business Process Change - Each organisation on the external sharing 'Allow List' must sign a Guest Partnering Agreement outlining their responsibilities. NHSmail sponsors of each federated group will receive an email every six months to make them aware that the group is still active and to request its removal if it is no longer required. Guest users will require the resource owner to approve an extension after the first 30 days of being granted access and after that, every 180 days.	Local Organisation	Guidance for NHSmail Guest Access	v4.61
			376	Existing Control: Design - The Local Administrator will receive a deletion success message when a guest user is removed.	Accenture	How guest inviters can delete and restore guest users via the NHSmail Portal	v4.61
			255	Existing Control: Business Process Change - The Local Administrator can remove O365 guest access that has been granted in error.	Local Organisation	How guest inviters can delete and restore guest users via the NHSmail Portal	v4.58

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Azure AD B2B Guest Access

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
126	Human Factor - Information sharing: The administrator does not manage guest access appropriately.	**v4.63**	249	Existing Control: Business Process Change - Guest access is controlled through the guest access extension process.	NHS England	Introduction to external user's guest access	v4.65.5
			370	Additional Control: Business Process Change - Local data sharing policies should be updated to include the monitoring of external guest access, e.g. through periodic guest access reviews.	Local Organisation	Manage guest access with Azure AD access reviews	v4.65.2
			830	Additional Control: Business Process Change - Local organisations can submit a Forensic Discovery Request where a Guest Access breach is suspected. This includes searching for content in 1:1 and 1:N chat conversations in which a guest user is a participant with other users in the organisation.	Local Organisation	Conduct an eDiscovery investigation of content in Microsoft Teams	v4.65.2
			259	Existing Control: Business Process Change - Sign-in activity will be monitored via an automated tracking process, and guest accounts that have not been logged into for 90 days will be deleted, and a new guest approval request will need to be submitted.	Accenture		v4.61

Application/Service Core O365 / Third-Party Applications

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
216	Business Process - Inappropriate information sharing/storage: Confidential patient information is accessed due to inappropriate sharing or storage.	**V4.65.2**	813	Existing Control: Design - Local Administrators can see the recent login details of the user accounts such as device name and time of the login attempts to the user accounts.	Local Organisation	Showing Recent Logons	v4.65.2
			366	Existing Control: Design - Data Loss Prevention (DLP) policies are used to control and protect patient confidential information when using O365 applications, including Exchange Online, SharePoint, OneDrive and Teams. Users will be prompted with a DLP pop-up when attempting to share sensitive information externally.	NHS England	Data Loss Prevention Guidance	v4.61
			605	Existing Control: Design - The Local Administrator can access an audit function that tracks any actions on the Portal that a Local Administrator or a User has performed, such as the action that was performed, who performed it, and the target object (e.g. user account) and the target organisation.	Local Organisation	Auditing actions	v4.63.3
			822	Existing Control: Business Process Change - All core O365 applications made available have been impact assessed by NHSE, and where data does not reside in the UK, these have been disabled by default, e.g. Whiteboard, Forms, Sway.	NHS England	O365 NHSmail Portal Management – Getting Started Guide	v4.65.2

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Core O365 / Third-Party Applications

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
216	Business Process - Inappropriate information sharing/storage: Confidential patient information is accessed due to inappropriate sharing or storage.	**V4.65.2**	811	Additional Control: Training - Guidance is provided on Data Loss Prevention, e.g. sensitivity flags, classifications and override feature.	NHS England	Data Loss Prevention Guidance	
			626	Existing Control: Training - Local organisations must adhere to the requirements of the Data Security and Protection Toolkit (DSPT). This requires all end-users to undertake annual Information Governance training (Standard 3). Training attendance is monitored, and an online knowledge test requires a minimum of 80% to pass, or a retest is required.	Local Organisation	Data Security Protection Toolkit	v4.63
			583	Existing Control: Business Process Change - End-users are expected to adhere to local IG policy and to report any suspected or known data breaches, including the accidental disclosure of confidential patient information.	Local Organisation		v4.64
			628	Additional Control: Business Process Change - A Forensic Discovery request can be used to investigate suspected data breaches. Details of the submission process are available on the NHSmail Portal help pages (must be approved by NHS England).	Local Organisation	Contact NHSmail Service Desk	v4.63
			555	Existing Control: Design - O365 two-factor authentication, single sign-on through Active Directory, and encryption of data in transit and at rest. Files are stored in SharePoint and are backed by SharePoint encryption.	Microsoft	Security and compliance in Microsoft Teams	v4.63
			821	Existing Control: Business Process Change - Each organisation should undertake a Data Protection Impact Assessment (DPIA) in conjunction with the published NHSmail Data Protection Impact Assessment and compliance with any existing local information governance policies. This should consider what O365 apps are made available locally and their acceptable use.	Local Organisation	NHSmail Information Governance Policies	v4.65.2
			823	Existing Control: Business Process Change - A review and approvals process has been defined, governed by the NHSmail Technical Design Authority (TDA), for integrating Microsoft, third-party or custom applications with the NHSmail Tenant.	NHS England	Application Hurdle Assessment	v4.65.6
			956	Additional Control: Business Process Change - End-user can manually apply Sensitivity Labels to classify and protect data, such as files and emails, as well as Groups and Sites. This will restrict what actions the recipient can perform on the data, such as editing or forwarding (this is an opt-in service).	Local Organisation	Sensitivity Labels Introduction	v4.69.2

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Core O365 / Third-Party Applications

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
216	Business Process - Inappropriate information sharing/storage: Confidential patient information is accessed due to inappropriate sharing or storage.	**V4.65.2**	896	Additional Control: Business Process Change - Local organisations should monitor end-user training compliance with the Data Security and Protection Toolkit training requirements.	Local Organisation	Data Security Protection Toolkit	v4.65.5
			897	Additional Control: Business Process Change - Local Organisations can configure additional DLPs to meet local IG policy and service requirements. Where the sender is allowed to override a DLP policy, this will be audited and should be monitored locally.	Local Organisation	Data Loss Prevention Guidance	v4.65.4
			910	Additional Control: Business Process Change - Local organisations can remove access to SharePoint and OneDrive during the period in which users can continue to access and use both applications (when the toggle switch is set to off).	Local Organisation	Disabling SharePoint & OneDrive Access	v4.65.2
			911	Additional Control: Training - Guidance is provided on the disabling of O365 applications.	NHS England	User Policy Management: Editing a policy	v4.65.2
			557	Existing Control: Design - Data Loss Prevention policies have been configured to protect sensitive information, e.g. can identify any document containing an NHS number stored in any OneDrive for Business or SharePoint site and prevent it from being shared.	NHS England	Data Loss Prevention Guidance	v4.63
			912	Additional Control: Business Process Change - Where end-users fail to adhere to acceptable use policies/guidance, the Local Administrators can disable individual O365 applications via the User Policy settings	Local Organisation		v4.65.5

Application/Service Egress Email Encryption

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
20	Human Factor - Email encryption requirement: End-user is unaware of the requirement to use email encryption when sending confidential patient information to a non-accredited or non-secure email or is unaware of how to use the encryption functionality.	**v4.61**	38	Additional Control: Business Process Change - Local organisations should monitor the use of email encryption within their organisation and take appropriate action where breaches are identified.	Local Organisation	Egress Investigate	v4.65.2
			690	Additional Control: Business Process Change - NHSmail encryption service has been communicated in the Local Administrator Bulletin, LA webinar and NHSmail Portal.	NHS England	New encryption service provider	v4.63

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Egress Email Encryption

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
20	Human Factor - Email encryption requirement: End-user is unaware of the requirement to use email encryption when sending confidential patient information to a non-accredited or non-secure email or is unaware of how to use the encryption functionality.	**v4.61**	505	Additional Control: Business Process Change - Local policy should require end-users to use encryption when sending email to non-secure domains.	Local Organisation	Data Security Protection Toolkit	v4.65.5
			37	Additional Control: Training - Guidance is provided on the user of email encryption, including how to apply the email secure encryption keyword tag and use of the Outlook 'Set Permissions' feature.	NHS England	Encryption Guide for NHSmail	v4.63
			331	Existing Control: Training - The Data Security and Protection Toolkit (DSPT) requires all end-users to undertake annual mandatory Information Governance training. The importance and methods used for protecting confidential patient information are covered, including email encryption. Training attendance is monitored, and an online knowledge test requires a minimum of 80% to pass, or a retest is required.	Local Organisation	e-Learning – data security awareness	v4.61
153	Human Factor - Plug-in unavailable: End-user cannot install the Egress encryption Outlook plug-in, or the plug-in is disabled, preventing the selection of the secure encryption classification from the 'set permissions' dropdown menu.	**v4.61**	326	Additional Control: Training - Guidance is provided on the minimum system, browser and device requirements needed to install the Egress Email Encryption and File Transfer Desktop Client.	NHS England	Encryption Guide for NHSmail	v4.61
			450	Additional Control: Training - Guidance is provided to support the installation of the Egress add-in.	NHS England	NHSmail Egress Outlook add-in	v4.63.2
			316	Existing Control: Business Process Change - If the Outlook plug-in is unavailable, the end-user can use the secure subject-line keyword encryption tag.	Local Organisation	NHSmail Egress Outlook add-in	v4.61
			315	Additional Control: Business Process Change - Local Organisation can use Group Policy to install the Egress Outlook plug-in and prevent users from disabling it.	Local Organisation	How to prevent users from disabling the Egress add-in	v4.61
155	Human Factor - Password management: End-user is unable to login to the Egress Web Access Portal as they have forgotten their login credentials.	**v4.61**	328	Existing Control: Design - Subject to local Active Directory Federation Service (ADFS) integration, end-users can authenticate to the Egress Outlook plug-in, Administration Panel and Web Access Portal using Single-Sign-On, removing the need to manage separate passwords and reducing the risk of password lockout	Accenture	Egress ADFS Configuration Guide (internal document)	v4.61

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Egress Email Encryption

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
155	Human Factor - Password management: End-user is unable to login to the Egress Web Access Portal as they have forgotten their login credentials.	**v4.61**	320	Existing Control: Business Process Change - Web Access Portal registration process requires users to set up security questions that can be used to perform a self-service password reset.	Local Organisation	How to update your password and security questions	v4.61
			321	Additional Control: Training - Guidance is provided on how to perform an Egress Web Portal password reset.	Egress	How to reset your password	v4.61
			319	Existing Control: Business Process Change - Egress provides Service Management support to assist with password reset, for example, if the user has forgotten the answers to their self-service password reset questions.	Egress	Support Centre	v4.61
157	Human Factor - Encryption keyword tag : End-user error in applying the subject line 'secure' keyword tag to the email.	**v4.61**	454	Existing Control: Design - Where encryption is used, this will be visible to the sender and recipient in the email body. The end-user can also access the Egress Administration Panel to view all emails where encryption has been applied or was intended.	Local Organisation		v4.63.2
			330	Additional Control: Training - Guidance is provided on how to apply the email encryption keyword tag.	NHS England	Encryption Guide for NHSmail	v4.61
			324	Existing Control: Design - The secure keyword tag business rule is not case sensitive and can be placed at any location within the email subject line.	NHS England		v4.61
206	Human Factor - Removal of secure keyword encryption tag from the email: End-user removes the secure encryption keyword tag from the email chain and forwards the email to one or more newly added email recipients.	**v4.61**	467	Existing Control: Design - If the secure encryption keyword tag is removed from an email chain and forwarded to a new recipient, encryption will be applied as if the tag was not removed.	Egress	Egress Protect	v4.61

Application/Service Email Gateway (Relay); Microsoft Safe Attachments

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
19	Technical - Virus scanning limitation: Encrypted attachments cannot be virus scanned by either the Relay service (Egress), or MS Safe Attachments (technical limitation), and as such, may contain malicious content, such as virus infected files.	**v4.72.3**	35	Additional Control: Business Process Change - Local organisations will be responsible for ensuring that they have a suitable risk mitigation method in place to detect malicious content that could be included in encrypted files.	Local Organisation	Data Security Protection Toolkit	v4.61

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Email Gateway (Relay): Microsoft Safe Attachments

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
19	Technical - Virus scanning limitation: Encrypted attachments cannot be virus scanned by either the Relay service (Egress), or MS Safe Attachments (technical limitation), and as such, may contain malicious content, such as virus infected files.	v4.72.3	1003	Additional Control: Training - Guidance is provided on the limitations of the security scanning functionality, including the scanning of encrypted content.	NHS England		v4.72.3

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
24	Technical - Malicious actor: Email system is targeted by external or internal intrusion attempts, e.g. phishing, impersonation attempt.	v4.70.2	816	Additional Control: Design - Local Organisation can configure email security protocols to reduce the risk of common cyber threats such as spoofing, phishing and malware.	Local Organisation	SPF, DKIM, DMARC Configuration	v4.65.2
			245	Existing Control: Design - O365 encrypts at rest and in transit, using several robust encryption protocols and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPsec), and Advanced Encryption Standard (AES).	Microsoft	Encryption	v4.57
			44	Additional Control: Business Process Change - Local Organisations can subscribe to Windows Defender ATP (opt-in service). WDATP can identify suspicious activity and take remedial action e.g. isolate workstation.	Local Organisation	Take response actions on a device	v4.61
			247	Existing Control: Design - There is a default MS policy to logout of O365 apps after 60 minutes.	Microsoft	Session timeouts for Microsoft 365	v4.65.2
			45	Additional Control: Business Process Change - NHSmail Acceptable Use Policy requires users to access their account from secure, encrypted devices that are password protected and lock unattended devices to ensure that data is protected in the event of the device being lost or stolen.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
			814	Existing Control: Training - Guidance is provided on how users can keep their accounts safe and secure from common cyber threats such as spam, junk, spoofing and phishing.	NHS England	How to identify common cyber threats	v4.65.2
			1051	Existing Control: Business Process Change - Detection of suspicious activity will automatically disable the user account and force remediation activities to be completed before it is reenabled, e.g. a password reset and enablement of Multi-Factor Authentication (MFA).	Accenture	Compromised Accounts	v4.76.2

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
24	Technical - Malicious actor: Email system is targeted by external or internal intrusion attempts, e.g. phishing, impersonation attempt.	**v4.70.2**	996	Additional Control: Business Process Change - Users can report spam or suspect phishing emails to spamreport@nhs.net for investigation by the NHSmail security team.	Local Organisation	Remain vigilant to Spam and Phishing Emails	v4.70.2
			997	Additional Control: Design - A free Trend "Phishing Reporter" plugin for Outlook is available to assist end-users in reporting phishing or spam emails to the NHSmail team. Organisations are advised to roll this out if they do not have a suitable alternative.	Local Organisation	Trend Micro Phishing Reporting Tool	v4.70.2
			990	Additional Control: Design - A MailTip will display specific safety tips to users when they receive an email from a sender that does not often email their account or emails for the first time.	NHS England	New anti-phishing safety tips	V4.70.2
25	Technical - Mobile device compromised: Data on the end-user mobile device is compromised, e.g. the device is hacked, data is unprotected at source or rooted device is used.	**v4.63**	784	Additional Control: Design - The NHSmail O365 Shared Tenant supports Microsoft Intune (opt-in) cloud-based mobile device management (MDM)/mobile application management (MAM) software. NHSE will apply default policies, and organisations can configure local policies and conditional access to control features and settings on Android, Android Enterprise, iOS/iPadOS, MacOS, and Windows 10 devices. Features include remote wipe, device lock, forced update to latest security patches, forced password reset, and device type restriction, e.g. corporate network limited to corporate devices.	Microsoft	Intune for Mobile Devices Early Adopters | Operations Guide	v4.65.5
			272	Additional Control: Training - Guidance is provided on mobile device security policies and the use of email encryption.	NHS England	Mobile Device Support Guide	v4.63.3
			197	Additional Control: Business Process Change - Local organisations should have policies in place outlining how to keep information secure when accessed on laptops or other computers outside of the organisation, including the need for all users to obtain approval to use a personal device (BYOD) with NHSmail.	Local Organisation	Bring your own device (BYOD) policy	v4.63.3
			86	Existing Control: Business Process Change - Local Administrators can monitor all mobile devices connected to an NHSmail account and, if necessary, can block access and erase data remotely .e.g. if the device is lost, stolen or otherwise compromised.	Local Organisation	Managing Mobile Devices	v4.65.2
			868	Additional Control: Design - Local Administrators can enforce the use of Multi-Factor Authentication when accessing NHSmail on a mobile device (User Policy Settings) or users can self-enrol to the MFA service.	Local Organisation	Multi-Factor Authentication (MFA)	v4.65.4

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
25	Technical - Mobile device compromised: Data on the end-user mobile device is compromised, e.g. the device is hacked, data is unprotected at source or rooted device is used.	**v4.63**	327	Existing Control: Business Process Change - The NHSmail Acceptable Use Policy, which all users have to accept before using the NHSmail service, stipulates that users should only access their account from secure, encrypted devices. These must be password protected, and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
27	Human Factor - Contact selection error: End-user error in selecting intended recipient contact details, e.g. email autocomplete feature error or selection of incorrect contact from the NHS Directory.		49	Additional Control: Business Process Change - Local email policy should cover contact selection and end-user responsibilities in reporting local data breaches.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
			416	Existing Control: Business Process Change - Egress email encryption allows emails sent to external users to be revoked or access to the email removed even after being sent/opened.	Local Organisation	Encryption Guide for NHSmail	v4.63.3
			489	Additional Control: Design - End-user can remove a name or email address from the Outlook Autocomplete List. The user or the local organisation can also deactivate this feature through a Group Policy or Registry change.	Local Organisation	Manage suggested recipients in the To, Cc, and Bcc boxes with Auto-Complete	v4.63.3
			415	Existing Control: Business Process Change - End-user can use the Outlook email recall feature to retrieve email from recipient mailboxes who have not yet opened it (both users must be on nhs.net).	Local Organisation	Recall an Email	v4.63.3
28	Human Factor - Shared Mailbox membership: User is added to a Shared Mailbox (SMB) in error, either by the Local Administrator during set-up or the SMB owner after its creation.	**v4.63.3**	499	Existing Control: Design - Only the Local Administrator can create a Shared Mailbox and set the initial permissions for its users. Following set-up, only the Shared Mailbox owner can add and remove members. To access a Shared Mailbox, each member must know the mailbox name, as they will need to search for the mailbox for it to appear. If they are assigned to a Shared Mailbox in error, it will not be apparent unless they are informed (it is impossible to log in to a Shared Mailbox directly, users must be added as members).	Microsoft	Setting shared mailbox permissions	v4.63.3
			501	Existing Control: Business Process Change - Local Administrators can submit Forensic Discovery Requests via the administration Portal to show if any confidential patient information has been disclosed. (NHS England must approve the request).	Local Organisation	Forensic Discovery Requests	v4.63.3
			509	Additional Control: Business Process Change - Local policy should require users to report mailbox membership errors to the local service desk.	Local Organisation		v4.63.3

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
28	Human Factor - Shared Mailbox membership: User is added to a Shared Mailbox (SMB) in error, either by the Local Administrator during set-up or the SMB owner after its creation.	**v4.63.3**	495	Additional Control: Training - Guidance is provided on creating and administering Shared Mailboxes.	NHS England	Administering Shared and Resource Mailboxes	v4.63.3
			886	Additional Control: Business Process Change - Whenever a Shared Mailbox is created or membership is changed, the mailbox Owner should verify that the details are correct.	Local Organisation		v4.65.4
38	Human Factor - Shared Mailbox misuse: Confidential patient information intended for only one individual member is sent or received by the shared mailbox.		490	Additional Control: Training - Guidance is provided on the appropriate use of Shared Mailboxes.	NHS England	Shared Mailbox Guide for NHSmail	v4.63.3
			493	Additional Control: Design - The Local Administrator can access an audit function that tracks any actions on the Portal that a Local Administrator or a User has performed, for example, the action that was performed, who performed it and the target object (e.g. user account) and the target organisation.	Local Organisation	Auditing actions	v4.63.3
48	Technical - Mobile device management: Encryption or password protection of mobile devices is not enforced and cannot be wiped remotely using native NHSmail Mobile Device Management features.	**v4.61**	740	Additional Control: Business Process Change - The use of a non-corporate device to access the NHSmail O365 Shared Tenant should only be done via the web interface and private/in browser mode to ensure that no sensitive information is cached on the device. Use on non-corporate devices is subject to local approval.	Local Organisation	Using NHSmail on shared computers or unmanaged devices	v4.64
			510	Additional Control: Business Process Change - Local organisations and federated partners are expected to ensure sufficient mobile device management capabilities where BYOD is permitted. Policies should include device encryption with an enforced password, minimum password length, inactivity timeout and a maximum number of failed password attempts, resulting in device wipe-out if exceeded.	Local Organisation	Bring your own device (BYOD) guidance	v4.61
269	Human Factor - Password policy: Weak password used, password compromised, e.g. shared by the user or stolen/leaked.	**v4.63**	687	Existing Control: Design - Complex password setting is enforced in line with National Cyber Security Centre (NCSC) guidelines, and password renewal is required every 365 days. Checks are also performed against previously compromised passwords (breached passwords are sourced from an internet-based breach database).	Accenture	NHSmail password policy	v4.65.5
			686	Additional Control: Business Process Change - Local organisation policy should include password security requirements.	Local Organisation	Data Security Protection Toolkit	v4.63

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
269	Human Factor - Password policy: Weak password used, password compromised, e.g. shared by the user or stolen/leaked.	**v4.63**	363	Existing Control: Design - An email account will be locked if it is suspected of becoming compromised, e.g. identified as sending a malicious email or login patterns do not match the user profile or would not be possible.	Microsoft	Risky Login Detection and Blocking	v4.63.3
			368	Additional Control: Training - Guidance is provided on password management and security.	NHS England	Reset your password	v4.63.3
			332	Existing Control: Business Process Change - End-users should not divulge their NHSmail password, and if stored electronically, this must be done following local policy.	Local Organisation		v4.63.3
			994	Additional Control: Business Process Change - Compromised accounts identified as being compromised will be disabled, and the passwords reset. MFA will also automatically be applied, which cannot be removed by the user.	Local Organisation	Compromised Accounts – Applying MFA	4.70.2
			995	Additional Control: Business Process Change - Local administrators should ensure that adequate validation of users is taking place when performing a password reset. Any reset done over the phone must include the validation of security questions.	Local Organisation		4.70.2

Application/Service Fast Identity Online (FIDO2)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
286	Human Factor - PIN compromised: FIDO security token PIN used to authenticate and access the NHSmail service has been shared by end-user.	**v4.65.6**	780	Additional Control: Training - Guidance is provided on protecting the security token PIN and what actions the user should take if they believe it has been compromised.	NHS England	FIDO2 Frequently Asked Questions (FAQs)	v4.65.6
			782	Additional Control: Business Process Change - Users should change their security token PIN from the old PIN received from Local Admins to a new PIN when they login for the first time.	Local Organisation	FIDO User Guide	v4.65.6
			781	Additional Control: Business Process Change - If a security token PIN has been compromised it can be removed by the Local Administrator and a new PIN can be set. The PIN can also be reset by the user through the Portal self-service facility.	Local Organisation	Contact NHSmail Service Desk	v4.65.6

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Fast Identity Online (FIDO2)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
321	Technical - FIDO2 set-up: Local Administrator is unable to set-up FIDO2 security token, e.g. unsupported browser/operating system.	**v4.65.6**	950	Additional Control: Testing - Test cases were executed using Chrome, IE, Firefox and Edge browsers in addition to OWA and Thick Client.	Accenture		v4.65.6
			951	Additional Control: Business Process Change - The Local Administrator can use MFA if FIDO cannot be set up..	Local Organisation	FIDO2 Admin Guide	v4.65.6

Application/Service Microsoft Intune

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
295	Human Factor - Company Portal Download: End-User is unable to install/run the Intune Company Portal App required to protect their device e.g. Intune licence not assigned (opt in service).	**v4.65.3**	844	Existing Control: Training - Guidance is provided on how to enrol end-user devices into the Intune service.	NHS England	Intune for Mobile Devices Early Adopters | Operations Guide	v4.65.3
			841	Existing Control: Training - Guidance is provided on how to download and run the Intune Company Portal App for each Mobile OS (iOS/Android).	NHS England	NHSmail Intune Service | Android Quick Start End User Guide and FAQ's	v4.65.3
			843	Existing Control: Business Process Change - End-users who are unable to complete the Intune enrolment tasks can contact their local service desk for assistance.	Local Organisation		v4.65.3

Application/Service Microsoft Outlook Calendar

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
30	Human Factor - Embedded attachments/free text: End-user embeds confidential patient information within the Outlook calendar invite, i.e., file attachment or as free text.	**v4.63**	53	Additional Control: Business Process Change - Local email policy should include reference to calendar management, that users must treat the contents of calendars with due care and consideration. This should align with the requirements of the NHSmail Acceptable Use Policy.	Local Organisation		v4.57
			52	Additional Control: Training - Guidance is provided on calendar federation, e.g. sensitive data should not be contained in the header or body of any calendar entries.	NHS England	Guidance to federate (share) calendars with NHSmail	v4.63

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Microsoft Outlook Calendar

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
30	Human Factor - Embedded attachments/free text: End-user embeds confidential patient information within the Outlook calendar invite, i.e., file attachment or as free text.	**v4.63**	933	Existing Control: Business Process Change - The NHSmail Acceptable Use Policy includes a section on end-user responsibilities when using the NHSmail calendar.	NHS England	NHSmail Acceptable Use Policy	v4.65.6

Application/Service Microsoft Safe Links/ Safe Attachments

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
338	Business Process - False negative: An email containing a URL or file attachment has been incorrectly classified as safe, and is not blocked, allowing the user to access a compromised application/file. (Note: this applies to external to nhs.net and nhs.net to nhs.net).	**v4.73.1**	1007	Existing Control: Business Process Change - Possible false negatives can be reported to the NHSmail help desk for investigation - helpdesk@nhs.net.	Local Organisation		v4.73.1
			1008	Additional Control: Business Process Change - If a false negative is reported, it will be reviewed by NHSE/CSOC and, if approved, can be added to the Tenant Allow and Block List (TABL).	NHS England		v4.73.1
			1033	Additional Control: Business Process Change - Microsoft will investigate false negative reports and, if verified, will update its pattern file to reclassify the URL as unsafe and block it (any TABL block can then be removed).	Microsoft		v4.73.1

Application/Service Microsoft Teams

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
39	Human Factor - Availability status: The assumption that an end-user displaying a Presence status as available is available. Information/guidance sent using an instant message to a user displaying an available presence is assumed by the sender as received/understood (applies to users communicating with NHSmail users and federated partners).	**v4.63**	568	Existing Control: Business Process Change - End-users should manually set the availability display status, e.g. 'Appear away' or 'Do not disturb', and specify a status message, such as a specific non-working day. The email out-of-office status will also display in the Teams application.	Local Organisation	Set your status message in Teams	v4.64
43	Human Factor - Permitted use: A&VC service is accessed by end-user who does not have authorisation to use the application.	**v4.61**	572	Existing Control: Business Process Change - End-users should comply with local password protection policies, they should not be shared, and if stored, this must be done securely and always following local IG policy.	Local Organisation		v4.64

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Microsoft Teams

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
43	Human Factor - Permitted use: A&VC service is accessed by end-user who does not have authorisation to use the application.	**v4.61**	710	Existing Control: Design - The NHSmail O365 Shared Tenant service enforces a complex password policy.	Accenture	Change your password	v4.63.3
			581	Additional Control: Business Process Change - The NHSmail Acceptable Use Policy, which all users have to accept before using the NHSmail service, outlines password management responsibilities. It includes never divulging password information and notifying the Local Administrator where unauthorised access is suspected. Local organisations should ensure that password protection policy includes reference to the NHSmail service and that compliance monitoring is undertaken regularly.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
46	Human Factor - Desktop sharing: User shares entire desktop, and information is unintentionally shown, which is not for the intended audience, e.g., leaving a previous session open when joining the next session.	**v4.61**	591	Additional Control: Training - Guidance is provided on the use of Teams A&VC, including considerations for clinical use, such as the recommended meeting settings to ensure that confidential patient data is protected.	NHS England	NHSmail Office 365 Clinical safety considerations	v4.64
			586	Additional Control: Business Process Change - End-users should ensure that before screen sharing, they have closed any documents, clinical programmes, browsers, and emails that may be confidential or sensitive (sharing only a specific application or a secondary monitor screen can help reduce this risk).	Local Organisation	Virtual Consultation	v4.64
			589	Additional Control: Business Process Change - Users should be aware that meeting attendees could take a screenshot of any shared content. Information of a sensitive nature should only be shared with a trusted audience.	Local Organisation		v4.64
86	Human Factor - Remote control: End-user gives remote access to their workstation.	**v4.63**	181	Additional Control: Design - Teams prompts external users to accept or reject requests to remote control when provided with the privilege by an external user. External users can revoke access at any time. NHSmail users are expected to use their judgement on the appropriateness of these features with external users.	Local Organisation	Share content in a meeting in Teams	v4.61
88	Human Factor - Attachment upload: Meeting attachments are uploaded to an externally hosted Teams meeting/conference containing confidential patient information that is accessed or stored inappropriately.	**v4.63**	183	Existing Control: Business Process Change - Users must manually choose to download attachments, the system does not automatically transfer them (Teams stores attachments in SharePoint).	Local Organisation	Using Files in Teams	v4.61

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Microsoft Teams

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
90	Human Factor - Recording storage: A&VC recordings containing Patient Confidential Data may be stored on a users personal device, local hard drive or cloud storage without appropriate security and control, e.g. file encryption, password protection or file/folder permissions (MS Stream uploading is currently disabled)	**V4.64.1**	186	Existing Control: Design - The Teams Call Recording toggle is enabled by default on all newly created User Policies but can be disabled by the Local Administrator via the Applications Settings box	Local Organisation	User Policy Management: Creating a policy	v4.45
			829	Additional Control: Design - Only the meeting organiser or person from the same organisation can initiate a meeting recording, i.e. not guest/external or anonymous attendee.	Microsoft	Recording Teams Meetings	v4.65.2
			708	Additional Control: Design - The Microsoft Stream uploading feature has been disabled, preventing recordings from being uploaded and inappropriately shared.	NHS England	Microsoft Stream	v4.63
			717	Additional Control: Business Process Change - Local organisations should undertake a Data Protection Impact Assessment, which should include the use of the Teams recording feature. In the absence of the Stream uploading feature, it is essential to ensure the secure storage of Teams recordings is specified.	Local Organisation	NHSmail Office 365 Teams deployment – information governance considerations	v4.65.2
92	Human Factor - Recording consent: Recording of confidential patient information without the consent of the meeting participants.	**V4.61**	187	Existing Control: Design - When the recording function is on, all meeting attendees will be notified via an on-screen 'recording' alert.	Microsoft	Recording Teams Meetings	v4.45
208	Business Process - Meeting attendee identification: Callers may access the A&VC meeting anonymously and/or identification of end-user may not be confirmed before commencing the meeting.	**V4.63.3**	819	Existing Control: Design - Meeting organisers can use the Teams meeting options to select attendees that can bypass the lobby and those who must be must be admitted. Teams can also be set to announce when a caller joins or leaves a meeting.	Local Organisation	Change participant settings for a Teams meeting	v4.65.2
			801	Existing Control: Design - Teams meetings organisers can download a meeting attendance list during the call (the report can only be downloaded during the meeting).	Local Organisation	Download Teams meeting attendance list	v4.65.2
			800	Existing Control: Design - A unique meeting will be generated for each Teams meeting on selecting 'Scheduling a Teams Meeting' (desktop app).	Microsoft	How to set up meetings	v4.65.2

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Microsoft Teams

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
260	Business Process - Storage of A&VC meeting files and notes: Documentation or notes made or received during A&VC meeting are not stored securely.	**V4.63.3**	561	Existing Control: Design - Teams data is encrypted in transit and at rest in Microsoft datacentres. Microsoft uses industry standard technologies such as TLS and SRTP to encrypt all data in transit between users' devices and Microsoft datacentres, and between Microsoft datacentres. This includes messages, files, meetings, and other content.	Microsoft	Security and Microsoft Teams	v4.64
261	Business Process - Unauthorised access to instant messages: Message chat may become compromised if the end-user device is not secure.	**v4.63.3**	563	Additional Control: Business Process Change - Where a data breach is suspected, Local Administrators can submit a Forensic Discovery Request via the NHSMail Portal (must be approved by NHS England). Teams e-discovery includes chat, messaging and files, meeting and call summaries.	Local Organisation	Security and compliance in Microsoft Teams	v4.65.5
			564	Additional Control: Business Process Change - Local organisations should ensure that where BYOD is permitted that the device is secured before access to confidential patient information is allowed. This should include, strong encryption for data in transmission, suitable authentication, hardware encryption for all data stored on the device and remote data erasure capability.	Local Organisation	Bring your own device (BYOD) guidance	v4.64
283	Human Factor - Message chat shared inappropriately: Confidential patient information accidentally shared in chat message with users who do not have a legitimate need to access the information.	**v4.63**	584	Additional Control: Business Process Change - Local Administrators can submit a Forensic Discovery Request via the NHSMail Portal (must be approved by NHS England). Teams e-discovery includes chat, messaging and files, meeting and call summaries.	Local Organisation	Security and compliance in Microsoft Teams	v4.65.5
			705	Additional Control: Design - The Team owner can remove members of a Team if they breach the terms of local/NHSmail Acceptable Use Policy.	Local Organisation	Remove someone from a team	v4.63
			543	Additional Control: Training - Guidance is provided on the use of the Teams chat feature, e.g. chat behaviour in private vs public channels and chat persistence.	NHS England	Start a Chat	v4.63.2
			544	Existing Control: Design - Microsoft uses Transport Layer Security to encrypt data in transit between user devices and Microsoft datacentres and includes messages, files, meetings, and other content.	Microsoft	Security and Microsoft Teams	v4.63.2
			706	Additional Control: Design - A separate Teams chat channel for private conversations can be used when sharing confidential patient information amongst users involved in the patient's direct care.	Local Organisation		v4.65.5

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Microsoft Teams

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
283	Human Factor - Message chat shared inappropriately: Confidential patient information accidentally shared in chat message with users who do not have a legitimate need to access the information.	**v4.63**	567	Additional Control: Business Process Change - Local organisations should have an IM&P policy detailing its acceptable use (based on the NHSmail Acceptable Use Policy) and that this is communicated to end-users, and compliance is regularly monitored.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
33	Human Factor - Delegate permissions: Inappropriate delegation of end-user mailbox.	**v4.63**	507	Additional Control: Training - Guidance is provided on delegating access to a mailbox/folder, e.g. how to delegate access and set permissions.	NHS England	Giving delegate access to your mailbox	v4.63
			62	Additional Control: Business Process Change - Local policy should include end-user responsibilities when delegating access to their mailbox/folders, e.g. restricting Read access to sensitive information to those with a legitimate reason to access it.	Local Organisation		v4.61
287	Human Factor - Public/Private Sharing: The end-user may unintentionally share patient sensitive information, e.g. O365 default app setting changed from private to public sharing. The former would be accessible to all NHSmail2 organisations (tenant wide). It would allow, for example, stored files to be viewed, edited and downloading.	**v4.65.2**	788	Additional Control: Training - Guidance is provided on privacy alerts, including the associated workflow and administrator responsibilities.	NHS England	O365 Privacy Monitoring	v4.65.2
			787	Additional Control: Design - If a user (resource owner) changes the default privacy setting from 'private' to 'public', (Teams/Site/Video Group), an email alert will be triggered to warn them of the consequence and to check the appropriateness. Local Administrators will also be alerted and will have access to a 'Privacy Configuration Report', allowing them to monitor privacy settings across the organisation or tenant, respectively.	NHS England		v4.65.2
			786	Additional Control: Business Process Change - Reminder communications regarding Public vs Private sharing when using O365 applications is provided in the LA Bulletin and Webinar sessions. This details the consequence of changing the default setting and outlines the responsibilities of organisations	NHS England	LA communication – 05 July 2021	v4.65.5

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Same Sign On

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
318	Technical - Password breach: Password is compromised, e.g. password is synchronised with an incorrect user, compromised password is synced or accessed during the sync process.	**v4.65.6**	940	Existing Control: Business Process Change - Organisations using the SSO service should configure their local password policy to align with the NHSmail complex password policy and enable the Fine Grain Password Filter to enforce the policy rules.	Local Organisation		v4.65.6
			941	Existing Control: Design - All password changes are encrypted in transit/rest, and access to the Sync Agent/Broker is subject to a service subscription and a valid certificate.	Microsoft		v4.65.6
			942	Additional Control: Business Process Change - Local organisations should have procedures in place for the secure storage of Public Key certificates.	Local Organisation		v4.65.6
			943	Additional Control: Testing - Integration product and performance testing will be undertaken on the bi-directional password synchronisation between the NHSmail and local (test org) Active Directories, error logging, security, password reset sync load testing and edge cases.	Accenture		v4.65.6

Application/Service Security Groups

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
348	Technical - Unauthorised resource access due to lack of automated JML process: The absence of an automated Joiners, Movers, and Leavers (JML) process in managing Security Group memberships allows users to retain access to resources from a previous organisation's Security Group.	**V4.78.1**	1058	Existing Control: Design - User activity is logged in the audit trail to ensure ongoing security and compliance monitoring.	Accenture		v4.78.1
			1057	Additional Control: Business Process Change - Administrators should conduct periodic manual audits to review Security Group memberships. The audit logging report feature can support this.	Local Organisation	Reporting for security groups	v4.78.1
			1055	Additional Control: Training - Guidance details crucial Security Group maintenance tasks for Local Administrators, including specific JML actions.	NHS England	Managing NHSmail Security Groups	v4.78.1

Hazard Event: The top event is the breach or loss of a significant volume of confidential patient data, affecting multiple individuals and causing widespread concern

Application/Service Tenant Allow/Block List (TABL)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
341	Technical - False negative: An external URL/domain/email address has not been identified as a threat and is not blocked, allowing the user to access malicious content. (Note: TABL is external to nhs.net only (does not apply to nhs.net to nhs.net messages); if the URL is not in the block list, then it is allowed).	**v4.73.1**	1034	Additional Control: Business Process Change - The Cyber Security Operations Centre (CSOC) ratifies the default TABL Global Policy block list with known threats. NHSE/CSOC will maintain the list, and should new threats be identified, they can add to the block list subject to approval. (Note: TABL will only need to be updated if Safe Links fails to detect the threat, e.g. a new attack vector).	NHS England		v4.73.1

HAZARD ID: H6 HAZARD: Unable to access encrypted content

Hazard Event: The top event is a prolonged period of inaccessibility to encrypted content that contains critical information needed for patient care and communication.

Key Hazard Assumptions 1.The user can login to their account.2.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available. **Linked Hazards:** H2:Disrupted communication and workflow due to NHSMail outage

Context: Emails sent to non-secure email domains must be encrypted. Security controls are used to manage access to encrypted emails and files, including a secure Web portal. The sender can remove access to the encrypted content before or after the content has been accessed.Global Sensitivity Labels can be added to emails, files, groups and sites to control what actions a user can perform on the data, e.g. read only, cannot forward.

Hazard Event: The top event is a prolonged period of inaccessibility to encrypted content that contains critical information needed for patient care and communication.

Cause/s: See possible caues below

Effect: Users cannot access important encrypted content such as patient data, emails, or shared documents. This could severely impact patient care and decision-making processes.

Harm: Potential patient harm may include delays in diagnosis or treatment due to the inability to access necessary patient information; errors in treatment due to missing or incomplete data; missed appointments or miscommunications due to inability to access email or scheduling information; and patient anxiety or stress caused by delays or lack of communication.

Service/s: Egress Email Encryption **Application/s:** Egress Web Portal **Subservice/s:** Egress Gateway

Category: Access **Hazard Status:** Open **Status Comment:** **Hazard Updated:** v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Egress Email Encryption

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
154	Human Factor - Account registration: Non-NHSmail user cannot complete the Egress Web account registration process, preventing them from creating, viewing, or responding to encrypted emails.	**v4.61**	318	Additional Control: Training - Guidance is provided on how to register for Egress Web Access	NHS England	Encryption Guide for NHSmail	v4.61
			317	Existing Control: Business Process Change - End-user registration account support will be provided by Egress during regular operating hours 08:30-18:00.	Egress	Egress Service Support	v4.61
			453	Existing Control: Design - The Egress user interface is intuitive and provides end-users with on-screen instruction on how to register for access to the Egress Web Access Portal	Egress	Egress Web Portal	v4.63.2
204	Human Factor - Egress Web Email access is revoked or expires: The sender revokes access to the email without warning, preventing the recipient from accessing its content, despite a legitimate need to do so. Access will also be denied if the email access expiry date is reached, but the recipient still needs to access the content.	**v4.61**	468	Existing Control: Design - The sender can reinstate access or extend the email access expiry date.	Local Organisation	Encryption Guide for NHSmail	v4.61
205	Human Factor - Single-Sign-On failure: End-user is unable to login to Egress encryption service using Single-Sign-On.	**v4.61**	459	Existing Control: Testing - Post-implementation testing is performed before SSO changes are released into the Production environment.	Accenture		v4.61

Hazard Event: The top event is a prolonged period of inaccessibility to encrypted content that contains critical information needed for patient care and communication.

Application/Service Egress Email Encryption

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
205	Human Factor - Single-Sign-On failure: End-user is unable to login to Egress encryption service using Single-Sign-On.	**v4.61**	458	Existing Control: Business Process Change - Local organisations should have a help desk function to resolve SSO access issues. If the help desk cannot provide resolution, a service incident can be raised with the NHSmail help desk.	Local Organisation	Contact NHSmail Service Desk	v4.61
			457	Existing Control: Training - Guidance is provided on the ADFS configuration of the Egress service.	Egress	Egress ADFS Configuration Guide (internal document)	v4.61

Application/Service Global Sensitivity Labels

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
327	Human Factor - Incorrect sensitivity label applied: The user applies an incorrect sensitivity label, preventing the recipient/s from editing, viewing or sharing the care information, e.g. internal label has been mistakenly applied to an externally bound email.	**v4.69.2**	969	Existing Control: Business Process Change - The application of sensitivity labels is not mandated. Labels applied in error can be removed by the owner subject to providing a justification reason.	Local Organisation		v4.69.2
			970	Additional Control: Training - Guidance is provided on the meaning, use, behaviour and known limitations associated with each data label.	NHS England	Sensitivity Labels Introduction	v4.69.2

Application/Service Trend Micro Email Encryption

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
203	Technical - Trend Micro encrypted email content: Emails encrypted using the legacy Trend Micro product may not be accessible to the end-user following migration to the Egress Email Encryption and File Transfer service.	**v4.61**	444	Existing Control: Design - Trend Micro Web Access Portal will continue to be available to end-users for read-only access of encrypted email content following migration to the Egress Email Encryption and File Transfer service.	Trend Micro		v4.61
			447	Additional Control: Business Process Change - Trend Micro will continue to provide end-user support to resolve account lockout issues (ready only access to legacy content) post migration to the Egress Email Encryption and File Transfer service.	Trend Micro	Contact NHSmail Service Desk	v4.63.2

HAZARD ID: H7 HAZARD: Unable to access NHSMail account

V4.82

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Key Hazard Assumptions 1.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.

Linked Hazards: H7:Unable to access NHSMail account; H8:Unable to access shared mailbox; H17:Accessing third-party (federated) applications

Context: Each user will have an account created by their Local Administrator, referred to as a User account. The User account is accessed via username and password. Multifactor authentication and Intune Mobile Device Management can also restrict access.

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Cause/s: See possible caues below

Effect: User cannot access their NHSmail account, impacting their ability to communicate and share important documents, despite the system being available.

Harm: Potential patient harm could include delays in communication of important health information, missed treatments due to lack of communication, potential for errors due to miscommunication, patient stress or anxiety due to delayed responses or lack of contact with healthcare providers, and potential for mismanagement of patient cases due to inability to access necessary information or communicate with other providers.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: Exchange Online; Outlook On The Web; Teams; SharePoint; OneDrive; Intune

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS); Azure Multi-Factor Authentication; Active Directory Federation Service

Category: Access

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Active Directory Federation Service

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
113	Human Factor - Single-Sign-On configuration: SSO access may be incorrectly configured on the Active Directory Federated Service.	**v4.57**	514	Existing Control: Business Process Change - Single-Sign-On Active Directory Federation Services configuration changes will be managed under the change control process and supported by post-implementation testing and back out plan.	Accenture		v4.57

Application/Service Azure Active Directory Connect

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
115	Technical - Active Directory synchronisation failure: Component failure or configuration error prevents synchronisation of the end-user objects.	**v4.63**	359	Existing Control: Design - Azure Active Directory (AAD) Connect uses both active (live sync) and standby servers (offline) to provide redundancy in the event of component failure	Microsoft	Azure AD Connect: Staging server and disaster recovery	v4.61
			230	Existing Control: Business Process Change - Service Management will provide synchronisation monitoring, including Health Monitoring (Sync status) \ Azure AD Connect Event Monitoring, changes to sync configuration, synchronising AD Domain Services infrastructure with the Azure AD and troubleshoot sync exceptions.	Accenture	Azure Active Directory Connect Health: Monitoring the sync engine	v4.63
162	Technical - Synchronisation of user details: Active Directory component failure or configuration error prevents synchronisation of the end-user attributes.	**v4.61**	346	Existing Control: Design - End-user details already synced to the Azure Active Directory will continue to be able to access O365 applications.	Microsoft		v4.61

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Azure Active Directory Connect

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
288	Technical - Sync Delay: A delay in the synchronisation process may prevent the user from accessing their account, e.g. password reset or account unlock.		233	Existing Control: Testing - Azure AD Connect synchronisation has undergone testing to verify that end-user object updates flow from the on-premise AD to Azure AD without incident. Any changes to the current service, e.g. group write-back feature, will also include regression testing.	Accenture		v4.63
			235	Existing Control: Design - A validation failure reason will be displayed on-screen to the end-user.	Accenture		v4.61
			789	Additional Control: Training - Guidance is provided on synchronisation timings.	NHS England	O365: Platform Sync Timings	v4.65.2
			834	Existing Control: Training - Guidance is provided on the Azure AD Connect Synchronisation Service.	NHS England	Azure AD Connect Sync	v4.65.2
			790	Existing Control: Design - Users already authenticated to Azure AD will continue to access the service for the remainder of the session (until log out).	Microsoft		v4.65.2

Application/Service Azure Identity Protection and Conditional Access

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
346	Business Process - Policy conflicts: Conditional Access Policies incorrectly identify legitimate users as high-risk, blocking them from accessing their account.	**V4.76.1**	1046	Additional Control: Business Process Change - Continuous monitoring is undertaken to identify false positives and remediate legitimate user accounts.	Accenture		v4.76.1
			1047	Additional Control: Testing - Testing has been undertaken on the configured policies to evaluate their impact before setting them live on Production.	Accenture		v4.76.1

Application/Service Azure Multi-Factor Authentication

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
301	Technical - MFA Server: MFA server failure prevents the processing of MFA requests, e.g. processes on the MFA backend leading to resource exhaustion to complete end-user authentication requests.	**v4.65.2**	861	Additional Control: Business Process Change - The Azure Active Directory Portal allows Service Management to view the Multi-Factor Authentication status reports to support the remediation of failed sign-ins.	Accenture	MFA sign-in report	v4.65.2

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Azure Multi-Factor Authentication

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
301	Technical - MFA Server: MFA server failure prevents the processing of MFA requests, e.g. processes on the MFA backend leading to resource exhaustion to complete end-user authentication requests.	**v4.65.2**	864	Existing Control: Design - Critical Azure components including Azure MFA have been designed to maintain high availability through redundancy and automatic failover to another instance with minimal disruption to service operations	Microsoft	How it works: Azure AD Multi-Factor Authentication	v4.65.2
			862	Additional Control: Testing - The Multi-Factor Authentication functionality has been tested to verify the resolution of authentication requests and MFA disable feature.	Accenture		v4.65.5
			860	Additional Control: Business Process Change - End-users can temporarily disable Multi Factor Authentication (MFA) for their account (MFA will be automatically reenabled after 15 minutes).	Local Organisation	Disabling MFA for your account	v4.65.2
			863	Existing Control: Design - A user who has already logged into the Portal before the Multi-Factor Authentication (MFA) outage can continue to use their account as they have already passed the authentication stage.	Microsoft		v4.65.2
302	Technical - Authentication Device: The end-user device that has been registered to receive the MFA verification code is unavailable, inactive or does not have network access.	**v4.65.2**	865	Existing Control: Design - The Microsoft Authenticator app runs on a smartphone or tablet, and once installed, does not require wi-fi or a mobile signal to generate a verification code.	Microsoft	Install Microsoft Authenticator App on your mobile (Android / iOS)	v4.67.1
303	Technical - Microsoft MFA app failure: The Microsoft MFA Authenticator app cannot be downloaded or fails to function.	**v4.65.2**	867	Additional Control: Training - Guidance is provided on Multi-Factor Authentication, including the methods available, registration, set-up and sign-in instructions	NHS England	Multi-Factor Authentication (MFA)	v4.65.2
			866	Additional Control: Design - NHSmail MFA policy allows the user to receive the verification code using several methods, including phone call and SMS.	Microsoft	Multi-Factor Authentication (MFA)	v4.65.5
304	Human Factor - Unreceived MFA code: The end-user requests the MFA verification code, but it is not received, or the user is unaware that it has been delivered	**v4.65.2**	875	Additional Control: Design - NHSmail MFA policy allows the user to receive the verification code using several methods, including phone call and SMS.	Microsoft	Multi-Factor Authentication (MFA)	v4.65.5
			859	Additional Control: Business Process Change - End-users should ensure that the notification settings on their mobile device are enabled to complete the authentication step promptly.	Local Organisation	Frequently asked questions (FAQ) about the Microsoft Authenticator app	v4.65.2

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Azure Multi-Factor Authentication

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
349	Human Factor - MFA Conditional Access Policy: A Local Administrator may mistakenly add a user from outside their organisation to an MFA Conditional Access Policy.	**v4.78.1**	1062	Additional Control: Business Process Change - Local Administrators should verify local Security Group users, reducing the risk of inadvertent inclusion in the organisation's MFA CA policy; an MFA Status report is available to support this process.	Local Organisation		v4.78.1
			1061	Additional Control: Training - Guidance materials on managing Security Groups and Named Locations have been provided to Local Administrators to facilitate effective policy implementation and maintenance.	NHS England	MFA Conditional Access	v4.78.1
			1060	Additional Control: Business Process Change - Before activating or modifying Conditional Access Policies that necessitate MFA, Local Administrators should communicate with all affected NHSmail users to ensure they are prepared for the change.	Local Organisation		v4.78.1
			1063	Additional Control: Business Process Change - The local administrator can remove users who have been mistakenly added into their organisation's Security Group.	Local Organisation		v4.78.1
			1059	Additional Control: Business Process Change - Local organisations should implement a change management process for NHSmail account Conditional Access Policies, integrating the existing JML protocol for permission management.	Local Organisation		v4.78.1
350	Business Process - NHS England MFA Policy Update: MFA by default: Effective 2nd October 2023, MFA will be the default for new User accounts, excluding PODS users. Some users may face challenges in setting up MFA.	**v4.79.1**	1065	Additional Control: Business Process Change - Local Administrators have the capability to disable Multi-Factor Authentication (MFA) for individual user accounts through the User Management page. This functionality should only be utilised as a last resort and under specific conditions to reduce the risk of account security.	Local Organisation	MFA Admin Guide	v4.79.1
			1029	Design: Training - NHSmail Portal help guidance inform users about MFA and how to set it up. Step-by-step guides and video tutorials is available to guide users through the MFA configuration process.	NHS England	Getting Started with MFA	v4.79.1
			1064	Additional Control: Business Process Change - Local Administrators should update local guidance for new starters to include MFA registration as part of setting up their NHSmail account.	Local Organisation		v4.79.1

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Care Identity Service (CIS2) Integration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
325	Technical - CIS2 authentication failure: The user cannot login to their account with their NHS Smartcard, e.g. Identity Agent configuration error; API failure; Identity matching service is unavailable; user incorrectly matched; performance issues; Browser/Client incompatibility.	**v4.75.1**	962	Existing Control: Design - The user must reauthenticate to initiate the pairing process. The matched accounts will be visible to the end-user before and after the linking process.	Accenture		v4.75.1
			961	Existing Control: Design - The CIS2 integration service is designed with high availability and active disaster recovery, e.g. regional load balancing and dynamic scaling. Key metrics will be monitored to ensure optimum performance, including latency, throughput, error rates and saturation metrics such as compute, network, and storage.	Accenture	Azure Monitor	v4.75.1
			960	Additional Control: Business Process Change - The service and associated guidance have been communicated via the LA Bulletin, LA Webinar (planned), and Portal comms.	Accenture	Information – NHSmail Services sign in page – Planned Upgrade	v4.75.1
			959	Additional Control: Testing - The NHSmail and CIS2 Integration service has been tested, including validation of API matching requests, exception handling, linking/unlinking, and authorisation (access) to NHSmail resources, e.g. Teams, OWA	Accenture		v4.75.1
			958	Existing Control: Business Process Change - If the user is unable to login to their NHSmail account or SSO application using their NHS Smartcard, they can revert to their original NHSmail identity's username and password.	Local Organisation		v4.75.1
			957	Additional Control: Training - End-user and LA guidance has been produced on the set-up, use and prerequisites for the CIS2 identity matching service.	NHS England	NHSmail & NHS Care Identity (Smartcard) Sign In | Frequently Asked Questions (FAQs)	v4.75.1
			963	Existing Control: Business Process Change - The user can unlink and relink incorrectly matched accounts.	Local Organisation	NHSmail & NHS Care Identity (Smartcard) Unlink Accounts | User Manual	v4.75.1

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Email Security

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
333	Business Process - Compromised account: The user mailbox account has been identified as compromised and has been disabled, blocking access to the user.	**v4.74.1**	1045	Additional Control: Training - The NHSmail Portal help pages include guidance on what actions a Local Administrator needs to follow to remediate an account marked as compromised.	NHS England	Compromised Accounts	v4.74.1
			1044	Additional Control: Business Process Change - The NHSmail helpdesk can remediate compromised accounts where the LA is unavailable, e.g. during out-of-hours for organisations covered by the National Administration Service.	Accenture		v4.74.1
			992	Additional Control: Business Process Change - Compromised accounts will be reenabled by the Local Administrator subject to a password reset and enablement of Multi-Factor Authentication. Note: any mailbox rules set up by the user will need to be re-activated by the user when the account is reenabled.	Accenture		V4.73.2

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
31	Human Factor - Password retry exceeded: End-user fails to enter correct username and password and (after 12 attempts) the account is locked.	**v4.64.2**	56	Existing Control: Business Process Change - Local Administrators can unlock an end-users account if they have forgotten their self-service password security questions or cannot access or use the password reset self-service facility.	Local Organisation	How to unlock a user's account	v4.61
			54	Additional Control: Business Process Change - End-users can quickly reset their password using the Portal self-service facility.	Local Organisation	Unlock your account	v4.61
			455	Additional Control: Training - Guidance is provided on end-user password management and account lockout.	NHS England	Getting ready to use self-service password reset and unlock	v4.61
131	Business Process - Password management: Invalid password/account lock out/expired password.	**v4.63**	271	Additional Control: Business Process Change - Local organisations should have a service desk function to enable end-users to report access issues. Local Administrators can reset passwords and unlock accounts on behalf of users. If the service desk cannot resolve, a service incident can be raised with the NHSmail help desk.	Local Organisation	Contact NHSmail Service Desk	v4.63
			903	Additional Control: Business Process Change - The local organisation should have a password policy that reminds users to change their password when reminded and not let it expire.	Local Organisation		v4.65.4

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
131	Business Process - Password management: Invalid password/account lock out/expired password.	**v4.63**	270	Existing Control: Training - Guidance is provided on the password reset process.	NHS England	Change your password	v4.63
			59	Existing Control: Business Process Change - 45-days before the password is due to expire, a password reminder email will be sent to the user at 18, 10, 5, 2 and 1 day(s). The user can change their password at any time during this period. The Self-Service password reset facility can be used to reset the password and unlock the account	Accenture	NHSmail password policy	v4.65.5
161	Human Factor - Account lockout: End-user has forgotten their login details or has locked their account.	**v4.61**	345	Existing Control: Design - Access to O365 is via Single-Sign-On, reducing the number of passwords that the end-user is required to manage.	Accenture	Single Sign-On Guide	v4.61
			344	Existing Control: Business Process Change - Accenture Service Management can assist Local Administrators who are unable to reset a users mailbox account.	Accenture	Contact NHSmail Service Desk	v4.64.2
			343	Existing Control: Business Process Change - End-user can use the self-service password function to reset their password.	Local Organisation	Self-service password reset not resetting password	v4.61

Application/Service Fast Identity Online (FIDO2)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
285	Human Factor - FIDO token not available: FIDO token used to authenticate and access the NHSmail service is unavailable, e.g. not allocated, lost, faulty, stolen, not registered to user, user has forgotten PIN.	**v4.65.6**	725	Additional Control: Business Process Change - Local organisations should have a process for reporting and replacing missing or defective tokens.	Local Organisation	FIDO User Guide	v4.65.6
			733	Additional Control: Business Process Change - A backup authentication method should be used, e.g. MS Authenticator App or second token, so that if the FIDO2 security token is unavailable, the account can still be accessed.	Local Organisation	Install Microsoft Authenticator App on your mobile (Android / iOS)	v4.65.6
			734	Additional Control: Training - Guidance is provided on how to register, reset and use the token.	NHS England	FIDO User Guide	v4.65.6

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Fast Identity Online (FIDO2)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
285	Human Factor - FIDO token not available: FIDO token used to authenticate and access the NHSmail service is unavailable, e.g. not allocated, lost, faulty, stolen, not registered to user, user has forgotten PIN.	**v4.65.6**	737	Additional Control: Business Process Change - A local support desk function should be available to deal with end-user troubleshooting requests, e.g. PIN reset and account unlock.	Local Organisation	Contact NHSmail Service Desk	v4.65.6
319	Human Factor - FIDO2 token locked: FIDO2 token locked: Security token has been locked due to the user exceeding PIN entry attempt limit (set to 8).	**v4.65.6**	946	Additional Control: Training - Guidance is provided on how to perform a PIN reset and manage blocked security tokens.	Local Organisation	FIDO2 Entering PIN Incorrectly	v4.65.6

Application/Service Managed Migrations

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
271	Business Process - Post-migration lockout: The user is unable to access their account post-migration, e.g. the O365 licence has not been enabled or user login credentials have not been preserved.	**v4.64.2**	747	Additional Control: Business Process Change - Service management can run a report to identify users of inaccessible Shared Mailboxes and unlock these proactively as a batch process, for example, where user permissions have not been migrated.	Accenture		v4.64.2
			745	Additional Control: Design - The Local Administrator can add an out of office message to the user account to inform the sender that the account is temporarily inactive and is not being actively monitored.	Local Organisation	Setting an out of office on behalf of a user	v4.64.2
			268	Existing Control: Testing - The migration tooling software used to perform the synchronisation of mailbox permissions have been successfully tested.	Accenture		v4.63
			267	Existing Control: Business Process Change - The local organisation will verify the migration of mailbox permissions during the pilot implementation phase.	Local Organisation		v4.63

Application/Service Microsoft Defender for Endpoint (MDE)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
11	Technical - User workstation isolation: MDE response action, e.g. isolation of end-user workstation by local organisation or NHS England Security Operations Centre.	**v4.57**	504	Additional Control: Business Process Change - Outlook Web App can be accessed on an alternative device should the Outlook Desktop Client be isolated by the local organisation or NHS England Security Operations Centre.	Local Organisation		v4.57

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Microsoft Intune

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
83	Business Process - Mobile device has been locked: The Intune policies/conditional access is misconfigured, preventing legitimate access to the end-user device (iOS/Android).	**v4.65.3**	711	Existing Control: Business Process Change - The Local Administrator should validate new and updated policies before their implementation to ensure that the enrolled device can be accessed by the end-user.	Local Organisation	Intune for Mobile Devices Early Adopters Operations Guide	v4.65.3
			839	Existing Control: Business Process Change - Where Mobile Device Management (MDM) / Mobile Application Management (MAM) policies have been set, the Local Organisation should ensure that a process is in place in the event that the end-user device or target application cannot be accessed, e.g. replacement device or change to policy settings.	Local Organisation		v4.65.3
			785	Existing Control: Testing - Testing has been undertaken on all default Intune policies.	Accenture		v4.65.3
			174	Existing Control: Business Process Change - End-users can report device/application access issues to their local help desk for resolution. If the Intune lockout issue cannot be resolved, access restrictions can be disabled by excluding the user from the policy [exclusions takes precedence over inclusion].	Local Organisation	Contact NHSmail Service Desk	v4.65.3
			840	Existing Control: Design - App configuration policies can be assigned to end-users before they run the app. The settings are then supplied automatically when the app is configured on the end-users device. End-users don't need to take action, reducing any risk of user error.	Microsoft	App configuration policies for Microsoft Intune	v4.65.3
297	Technical - Passcode Lockout: End-user device enrolled into the Intune service has been locked, e.g. user unable to recall passcode.	**v4.65.3**	845	Additional Control: Training - Guidance is provided on resetting the Intune passcode.	NHS England	Intune for Mobile Devices Early Adopters | Operations Guide	v4.65.5

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
190	Human Factor - Deletion of NHSmail account: End-user account is accidentally deleted. This may be caused by an error during the bulk deletion process or it may be marked with a leaver status by the Local Administrator or joiner, mover, leaver (JML) synchronisation process, resulting in its deletion after 30 days if not picked up by a new organisation.	**v4.63**	9	Existing Control: Business Process Change - Changes are tested in a pre-production environment for any adverse impact on service performance before migration to the Production environment.	Accenture		v4.61

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
190	Human Factor - Deletion of NHSmail account: End-user account is accidentally deleted. This may be caused by an error during the bulk deletion process or it may be marked with a leaver status by the Local Administrator or joiner, mover, leaver (JML) synchronisation process, resulting in its deletion after 30 days if not picked up by a new organisation.	**v4.63**	603	Additional Control: Business Process Change - For the first 30 days after deletion the account can be restored by the Local Administrator. Once an account has been deleted, it is recoverable for a further six months (180 days) through a request to help-desk@nhs.net (this must be supported with a compelling business case).	Local Organisation	Contact NHSmail Service Desk	v4.63
			602	Existing Control: Design - The system has been configured to send the end-user an email notification as soon as the Local Administrator has marked their account with the status of 'Leaver'.	Accenture	Marking a user as a Leaver	v4.63
			431	Existing Control: Business Process Change - For the first 30 days after deletion the account can be restored by the Local Administrator. Once an account has been deleted, it is recoverable for a further six months (180 days) through a request to help-desk@nhs.net (this must be supported with a compelling business case).	Accenture	Delete or Restore a User Account	v4.61
			432	Existing Control: Business Process Change - An email will be sent to all end-users in scope for deletion, after which the users will have up to 14 days to take the necessary action specified in the email to prevent it from being deleted.	Accenture		v4.63
			433	Existing Control: Testing - End-user mailbox SQL communication and deletion scripts are tested in a pre-production environment to ensure that the communication emails are sent to the correct End-user mailboxes and that the account deletion script works as intended. The test evidence is submitted to NHS England as part of the RFC process.	Accenture	Deletion of Inactive, Active Leaver, Disabled Leaver and Disabled Accounts (standard internal RFC)	v4.61
			13	Existing Control: Business Process Change - End-users will be given at least 14 days' notice before an inactive mail account is deleted. If the user logs into their account during this period, e.g., sending an email, the system will automatically reset the account to active.	Accenture	Types of Account Status	v4.63

Hazard Event: The top event is a sustained period where a user cannot access their NHSmail account while the overall infrastructure, such as servers and network connections, is functioning normally

Application/Service Same Sign On

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
317	Technical - Password Synchronisation Failure/Delay: Sync failure/delay of the NHSmail and local Active Directories, e.g. sync agent/broker misconfiguration, password policy misalignment, certificate expiration, password Sync Broker overload/downtime, TANSync delay, e.g. new user creation, in addition to Local Security Authority (LSA) policies.	**v4.68.1**	935	Additional Control: Business Process Change - Local organisations should communicate the Same-Sign-On service to their end-users, specifically the steps that should be followed in the event of login failure.	Local Organisation	Same Sign On Communications Template	v4.68.1
			936	Additional Control: Training - Onboarding guidance is provided detailing the local organisation set-up actions, e.g. technical pre-requisites and sync agent password installation and validation. Troubleshooting guidance is also provided, e.g. potential password history conflicts and additional AD security policies that may affect sync actions between the NHSmail AD and local AD.	NHS England	Same Sign On Onboarding Guide	v4.68.1
			937	Additional Control: Testing - Following the installation of the password sync agent, the local organisation should perform a password change to verify that the user can access their NHSmail and local accounts.	Local Organisation		v4.65.6
			938	Existing Control: Design - The Sync Broker is highly available and resilient to network or agent downtime. The service can scale in line with service demands, and in the event of unscheduled downtime, messages will queue until the endpoint is restored	Microsoft		v4.65.6
			939	Additional Control: Business Process Change - Local organisation should have procedures in place to manage their public certificate renewal (SSO certificate expires every 2 years).	NHS England	Same Sign On Onboarding Guide	v4.65.6
			952	Additional Control: Training - Guidance is provided on Same Sign On sync delay scenarios, e.g. newly created users, including what actions a user must take to enable the password synchronisation.	NHS England	Change your password	v4.66.1
			934	Additional Control: Testing - Integration product and performance testing will be undertaken on the bi-directional password synchronisation between the NHSmail and local (test org) Active Directories, error logging, security, password reset sync load testing and edge cases.	Accenture		v4.65.6

HAZARD ID: H8 HAZARD: Unable to access shared mailbox

V4.82

Hazard Event: Inability to access the shared mailbox due to permission issues or technical problems

Key Hazard Assumptions 1.The user can login to their account.

Linked Hazards: H7:Unable to access NHSmail account

Context: A Shared Mailbox is used to send and receive emails on behalf of a team. It is created by a Local Administrator and must have an owner assigned. Members can be added to the mailbox, and mailbox permissions, such as read/send, can be controlled by the owner.

Hazard Event: Inability to access the shared mailbox due to permission issues or technical problems

Cause/s: See possible caues below

Effect: Unable to send and receive clinical information, e.g. discharge summaries, medication records and referrals.

Harm: Disrupted communication, delayed response to emails, potential for missed important emails or updates, potential impact on workflow and productivity, potential for miscommunication or incomplete information sharing within the team, which could indirectly impact patient care and safety through delayed or inaccurate decision-making, compromised coordination, or missed critical updates.

Service/s:

Application/s:

Subservice/s:

Category: Access

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Low **Initial Clinical Risk:** 2 - Low

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
308	Business Process - Shared Mailbox delegate permissions: The delegated permission have not been migrated to the Shared Mailbox.	**v4.65.4**	900	Additional Control: Business Process Change - Local organisations should have business continuity measures in place in the event that more team members cannot access a Shared Mailbox.	Local Organisation		v4.65.4
			899	Existing Control: Business Process Change - Shared Mailbox permissions will be migrated.	Accenture		v4.65.4
			901	Additional Control: Business Process Change - Post-migration, each member of the Shared Mailbox should verify that they are able to access the mailbox and that their permissions have been preserved in full.	Local Organisation		v4.65.4
309	Human Factor - Shared Mailbox deletion: The Shared Mailbox has been deleted by the owner, Local Administrator or mailbox hygiene process (a Shared Mailbox with an inactive status will be eligible for deletion).	**v4.65.4**	878	Existing Control: Business Process Change - A Shared Mailbox that has been deleted can be restored by the Local Administrator within a 30 day period (after 30 days it will need to be recreated).	Local Organisation	Deleting and restoring a shared mailbox	v4.65.4
			422	Additional Control: Business Process Change - Shared mailbox owners should inform the relevant National Administrative Service (NAS) team where colleagues are on long-term absence to request the account is disabled – a request should then be made to enable the account upon the user's return to work.	Local Organisation	National Administration Service (NAS) contacts	v4.61

HAZARD ID: H8 HAZARD: Unable to access shared mailbox V4.82

Hazard Event: Inability to access the shared mailbox due to permission issues or technical problems

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
309	Human Factor - Shared Mailbox deletion: The Shared Mailbox has been deleted by the owner, Local Administrator or mailbox hygiene process (a Shared Mailbox with an inactive status will be eligible for deletion).	**v4.65.4**	881	Additional Control: Business Process Change - Shared Mailbox owners should send an email at least once within a six month period to avoid being marked as inactive and identified for deletion.	Local Organisation	Mailbox Hygiene Design (internal document)	v4.65.4
			884	Additional Control: Training - Guidance is provided on Shared Mailbox statuses that are applied in the NHSmail Portal.	NHS England	Shared Mailbox Statuses	v4.65.4
			423	Existing Control: Design - End-user will receive an on-screen prompt and be required to confirm the deletion of the Shared Mailbox, reducing the risk of accidental removal. If deleted in error, the mailbox can be restored if done within 30 days.	Accenture	Deleting and restoring a shared mailbox	v4.61
311	Business Process - Shared mailbox provisioning: Mailbox provisioning processing delays prevent access and ability to undertake user membership tasks.	**v4.65.4**	877	Additional Control: Training - Guidance is provided on creating a Shared Mailbox, including possible provisioning delays.	NHS England	Creating a shared mailbox	v4.65.4
312	Human Factor - Shared mailbox membership: The user has not been added to the Shared Mailbox.	**v4.65.4**	887	Existing Control: Business Process Change - The mailbox Owner can add a user to the Shared Mailbox once the account has been created and Owner assigned.	Local Organisation	Time delay in removal of Shared Mailbox ownership rights	v4.65.4
			879	Existing Control: Design - When attempting to delete a Shared Mailbox, a confirmation pop-up will be displayed, minimising the risk of accidental deletion.	Local Organisation	Deleting and restoring a shared mailbox	v4.65.4

HAZARD ID: H9 HAZARD: Guest and external users unable to access shared resources

V4.82

Hazard Event: Configuration issues or network connectivity problems

Key Hazard Assumptions 1.The user can login to their account.

Linked Hazards: H7:Unable to access NHSmail account

Context: Where locally approved, Guest access enables users outside the organisation to collaborate with users from other organisations, e.g. become a member of a team and participate in team chat. External access lets users find, call, chat, and set up meetings with your team members in other domains (may be subject to local/tenant restrictions).

Hazard Event: Configuration issues or network connectivity problems

Cause/s: See possible caues below

Effect: Restricted collaboration, hindered communication, delays in information sharing and workflow due to limited access for guest and external users.

Harm: Failing to routinely monitor user/shared mailboxes can indirectly impact patient care by delaying critical updates, compromising timely decision-making, and disrupting care coordination among healthcare professionals, such as multidisciplinary teams (MDTs). These delays and disruptions can potentially lead to adverse clinical outcomes for patients.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: Teams; SharePoint; Microsoft One Drive For Business

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Access

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Azure AD B2B Direct Connect

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
339	Human Factor - Information Sharing: Azure Direct Connect access has been incorrectly set up.	v4.80.1	1031	Additional Control: Testing - To confirm the enforcement of access controls and restrictions, the B2B Direct Connect configuration underwent testing in a pre-production environment, using a temporary M365 tenant to simulate an external partner organisation.	Accenture		v4.80.1

Application/Service Azure AD B2B Guest Access

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
165	Technical - Guest access expiry: Guest access has expired.	v4.61	354	Additional Control: Training - Guidance is provided on the guest access extension process.	NHS England	Introduction to guest access process and capabilities	v4.65.5
			892	Additional Control: Business Process Change - Local organisations should have a process to manage the timely approval of guest accounts (guests will require approval for an extension after the first 30 days of being granted access every subsequent 180 days).	Local Organisation		v4.65.2
			225	Existing Control: Business Process Change - A notification email will be sent to the Local Administrator before the expiry of the O365 licence.	Microsoft		v4.61

Hazard Event: Configuration issues or network connectivity problems

Application/Service Azure AD B2B Guest Access

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
165	Technical - Guest access expiry: Guest access has expired.	**v4.61**	812	Additional Control: Design - The Local Administrator can run a O365 Licence Report, which includes the expiry date of all O365 licences assigned by the organisation.	Local Organisation	Admin Reports	v4.65.2
166	Business Process - Guest access: Guest access has not been approved, activated or has been revoked.	**v4.61**	355	Additional Control: Design - Guest access not approved before expiry will be immediately revoked, and the Guest User will need to be re-invited, and data will need to be shared again.	Microsoft		v4.61

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
168	Human Factor - Guest Active Directory: Local Administrator has not set up guest account.	**v4.61**	351	Additional Control: Training - Guidance is provided on the set up of Azure Federated Groups set for External Organisations.	NHS England	Azure Federated Groups	v4.61
169	Human Factor - External Allow List: Local Administrator has not added guest organisation to the external organisation Allow List.	**v4.61**	358	Existing Control: Business Process Change - Local Administrators can raise an external organisation domain allow-list request to the Live Service Team from within the Portal.	Local Organisation	Create a guest access allow list request	v4.61

HAZARD ID: H10 HAZARD: Unable to administer user accounts

V4.82

Hazard Event: Local and Primary Administrators unable to administer service.

Key Hazard Assumptions 1.The user can login to their account.2.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.

Linked Hazards: H2:Disrupted communication and workflow due to NHSmail outage; H7:Unable to access NHSmail account

Context: The Portal administrator logs into their account using a username and password. They must then also authenticate using Azure Multi-Factor Authentication.

Hazard Event: Local and Primary Administrators unable to administer service.

Cause/s: See possible caues below

Effect: Inability to conduct account management, password resets, set user permissions, security management, and troubleshooting/support.

Harm: May result in delayed access to critical patient information, potentially resulting in indirect harm by impacting timely diagnosis and treatment.

Service/s: Portal **Application/s:** Exchange Online **Subservice/s:** Amazon Web Services (IaaS); Azure Multi-Factor Authentication

Category: Account Administration **Hazard Status:** Open **Status Comment:** **Hazard Updated:** v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Azure Multi-Factor Authentication

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
186	Technical - MFA server: MFA server failure prevents the processing of MFA requests, e.g. processes on the MFA backend leading to resource exhaustion to complete end-user authentication requests.	v4.61	58	Additional Control: Business Process Change - Users can temporarily disable Multi Factor Authentication (MFA) for their account (MFA will be automatically reenabled after 15 minutes).	Local Organisation	Disabling MFA for your account	v4.65.7
			434	Existing Control: Design - A Local Administrator who has already logged into the Portal before the Multi-Factor Authentication (MFA) outage can continue to use their account as they have already passed the authentication stage.	Accenture		v4.61
			216	Existing Control: Business Process Change - Azure Active Directory Portal allows Service Management to view the Multi-Factor Authentication status reports to support failed sign-ins.	Accenture	MFA sign-in report	v4.57
			217	Existing Control: Testing - The Multi-Factor Authentication functionality has been tested to verify the resolution of authentication requests. The disabling of MFA enabled access to the Portal without needing the authenticate.	Accenture		v4.65.5
			672	Existing Control: Design - Critical Azure components including Azure MFA have been designed to maintain high availability through redundancy and automatic failover to another instance with minimal disruption to service operations.	Microsoft	How it works: Azure AD Multi-Factor Authentication	v4.63

Hazard Event: Local and Primary Administrators unable to administer service.

Application/Service Azure Multi-Factor Authentication

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
192	Technical - Verification code: MFA verification code is requested but not received.	**v4.61**	604	Additional Control: Business Process Change - End-users should ensure that the notification settings on their mobile device is enabled so that phone calls, messaging app, or authentication app (Microsoft Authenticator), sends the alerts. (push notifications are not required, but they are a helpful alert and help ensure that the verification method is completed quickly).	Local Organisation	Frequently asked questions (FAQ) about the Microsoft Authenticator app	v4.63
195	Technical - Authentication device: The end-user device that has been registered to receive the MFA verification code is unavailable, inactive or does not have network access.	**v4.61**	673	Existing Control: Design - The Microsoft Authenticator app runs on a smartphone or tablet, and internet access or mobile services are not required to receive the verification code.	Microsoft	Install Microsoft Authenticator App on your mobile (Android / iOS)	v4.65.5
196	Technical - MFA configuration: The Microsoft MFA Authenticator app cannot be downloaded or fails to function.	**v4.61**	607	Additional Control: Design - NHSmail O365 Shared Tenant MFA policy allows the user to receive the verification code using several methods, including phone call and SMS.	Microsoft	Multi-Factor Authentication (MFA)	v4.65.5
			674	Additional Control: Training - Guidance is provided on the set up and use of Multifactor-Authentication.	NHS England	Multi-Factor Authentication (MFA)	v4.63

HAZARD ID: H11 HAZARD: User does not routinely monitor their user/shared mailbox

V4.82

Hazard Event: User and shared mailboxes are not routinely monitored

Key Hazard Assumptions 1.The user can login to their account.

Linked Hazards: H7:Unable to access NHSmail account

Context: Users must regularly monitor user and Shared mailboxes to ensure that care information is promptly actioned and ensure that the account remains in an active state. Account activity is monitored, and inactive accounts will be removed from the service.

Hazard Event: User and shared mailboxes are not routinely monitored

Cause/s: See possible caues below

Effect: Delayed or missed communication, missed referrals or consultations, medication errors or discrepancies, incomplete patient records, unaddressed patient concerns.

Harm: Failing to routinely monitor user/shared mailboxes can result in delayed diagnosis and treatment, causing heightened patient anxiety and potentially exacerbating their health conditions.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: Exchange Online; Outlook On The Web

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Account Administration

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
82	Human Factor - User account monitoring: User/Shared Mailbox is not routinely monitored.	v4.61	417	Additional Control: Business Process Change - Users should indicate when their mailbox is not being monitored by using the out-of-office feature, including an alternative point of contact wherever possible.	Local Organisation		v4.65.2
			517	Additional Control: Business Process Change - Users can access their email from mobile devices on different platforms, making it easier to stay connected and maintain their mailbox.	Local Organisation	Mobile Device Support Guide	v4.65.1
			902	Additional Control: Design - When the recipient adds an out-of-office reply, the sender will be notified following delivery of the email and a MailTip will also warn the sender at the point of composing the email.	Microsoft	MailTips	v4.64.4
			173	Additional Control: Business Process Change - When sending sensitive information, users should always request a delivery and read receipt (Email) or recipient acknowledgement (Instant Messaging) to verify that the information has been received. This is especially important for time-sensitive information such as referrals.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
			222	Additional Control: Business Process Change - If the user is unable to manage their mailbox effectively, it can be delegated.	Local Organisation	Giving delegate access to your mailbox	v4.65.1

Hazard Event: User and shared mailboxes are not routinely monitored

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
82	Human Factor - User account monitoring: User/Shared Mailbox is not routinely monitored.	**v4.61**	685	Additional Control: Training - Guidance is provided on the setting of automatic replies (Out of Office) by the user and on behalf of a user (Shared Mailboxes, the Owner must set the Out of Office).	NHS England	Setting automatic replies (Out of Office)	v4.63

HAZARD ID: H12 HAZARD: Updating patient care records; user fails to update the patient care record or updates it with delay

V4.82

Hazard Event: User fails to update the patient care record or updates it with delay.

Key Hazard Assumptions 1. User can access the patient care record system.

Linked Hazards: None Recorded

Context: The lack of interoperability between health and care organisations means that NHSmail is used to transmit patient data at scale. The NHSmail O365 Shared Tenant is not integrated into the patient care record and requires end-users to transfer patient data to the care record manually.

Hazard Event: User fails to update the patient care record or updates it with delay.

Cause/s: See possible caues below

Effect: Incomplete or outdated patient care information, potential errors or omissions in treatment plans or medication orders, delayed access to critical patient information, compromised care coordination due to missing or delayed updates, increased risk of duplicate or conflicting documentation

Harm:

Delayed or neglected updates to patient care records can lead to potential harm. Failure to promptly update the records can result in outdated or inaccurate information, which can impact the quality and continuity of patient care. Healthcare providers relying on outdated records may make incorrect treatment decisions, prescribe inappropriate medications, or overlook critical patient information. This can lead to compromised patient safety, delayed interventions, and suboptimal healthcare outcomes.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: Exchange Online; Outlook On The Web

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Record Keeping

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Major **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Major **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Microsoft Office 365 Online (SaaS): Exchange Online

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
220	Human Factor - Misuse of NHSmail: End-user does not update the patient care record and may use their email account/O365 application as an extension to the patient health record, e.g., an archive facility.	V4.63	658	Additional Control: Business Process Change - Health Practitioners have a duty to keep up to date with, and adhere to relevant legislation, case law, Professional Bodies and professional standards, national and local policies relating to information governance and record keeping standards.	Local Organisation	The Common Law Duty of Confidentiality	v4.63
			530	Additional Control: Business Process Change - Local organisations should have a policy on record-keeping, including the transcription of electronic communications. This should be communicated, and adherence monitored through local audit.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
			534	Additional Control: Business Process Change - Federation Partners will be required to sign a Federation Partner Agreement detailing their responsibilities. This agreement includes ensuring that an appropriate Acceptance Use Policy (AUP) ensures that their users appropriately document any clinical communications.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6

HAZARD ID: H13 HAZARD: Legitimate emails and attachments are quarantined and/or deleted (false positive)

V4.82

Hazard Event: Legitimate emails and attachments are quarantined and/or deleted (false positive).

Key Hazard Assumptions None Recorded

Linked Hazards: H4:Inability to Send or Receive Emails and Attachments

Context: The email network is continually monitored for security threats using filtering rules to quarantine and, if necessary, delete suspicious emails and URL links. A Tenant Global Policy Allow and Block List (TABL) is also used to prevent access to specific content, and these rules may prevent users from accessing legitimate emails, domains or URLs.

Hazard Event: Legitimate emails and attachments are quarantined and/or deleted (false positive).

Cause/s: See possible caues below

Effect: Misplaced or lost important communication and attachments, missed critical information or instructions, delayed access to time-sensitive information, disruption of workflow and communication, increased risk of miscommunication or misunderstanding.

Harm: Indirect patient harm may occur due to delayed diagnosis, treatment, or response to urgent medical needs. Inadequate follow-up or monitoring may arise, causing delayed or missed appointments and suboptimal patient management. Furthermore, patient concerns or requests may go unaddressed, leading to dissatisfaction, worsening symptoms, or neglected medication refills.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: Exchange Online; Outlook On The Web

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS); Trend Cloud Application Security (SaaS)

Category: Performance

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
64	Human Factor - Email Gateway configuration: Configuration error within the NHSmail Email Gateway service may impact email flow.	v4.61	894	Existing Control: Design - A MailTip will notify the sender of recipients accounts that are being moderated and may be subject to a delay in delivery.	Microsoft	MailTips	v4.65.4
			462	Existing Control: Business Process Change - All changes to the NHSmail O365 Shared Tenant encryption business rules are done under change control, including formal approval (Accenture and NHS England) and testing in a pre-production environment before release into live service.	Accenture		v4.65.2
			123	Existing Control: Business Process Change - Local organisations should have a support desk function to enable end-users to report mail flow issues, e.g. false positives. This should include an escalation process to the NHSmail helpdesk.	Local Organisation	Contact NHSmail Service Desk	v4.61
			122	Additional Control: Business Process Change - Users should request an email delivery/read receipt where sensitive information is communicated. A Non-Delivery Receipt (NDR) will be sent to the sender should the email fail to reach its destination.	Local Organisation	Requesting a read or delivery receipt	v4.61

Hazard Event: Legitimate emails and attachments are quarantined and/or deleted (false positive).

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
66	Technical - False positives: The email Gateway security filters blocks or delays the exchange of legitimate email (false positive).	**v4.63**	131	Existing Control: Design - An end-user that is blocked on the Relay due to their account being compromised (reputational filtering) will be alerted by email and advised to contact their Local Administrator to restore the account.	Accenture	Deny-Listing – Email sent to external recipients (e.g. Gmail / Hotmail / Outlook.com) may be blocked or delivered to junk	v4.61
			832	Additional Control: Training - Guidance is provided on Junk Mail management and the Minimum Dataset for submitting a false positive report to the NHSmail service desk.	NHS England	Junk Mail Guidance Update	v4.65.2
			810	Additional Control: Training - Guidance is provided on Non Delivery Reports (NDRs).	NHS England	Non Delivery Reports (NDRs)	v4.65.2
			831	Additional Control: Business Process Change - When a legitimate email has been categorised as junk, and there are no wider configuration issues (SPF, DKIM, DMARC), the Local Administrator (or end-user) should provide a sample of the email so that the Service Management team can submit a false-positive case.	Local Organisation	Contact NHSmail Service Desk	v4.65.2
			124	Additional Control: Business Process Change - Local email policy should align with the NHSmail AUP and stipulate the use of delivery and read receipts when emailing sensitive and time sensitive information, e.g. patient referral.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
			726	Existing Control: Business Process Change - Local organisations should have procedures in place to confirm email receipt where Non-Delivery Receipts are not used or supported.	Local Organisation		v4.64.2
			130	Existing Control: Design - Trend Micro employs many highly effective techniques to reduce the number of legitimate emails that inappropriately quarantined, including Machine Learning and reputation filtering.	Trend	Enterprise Security Solutions	v4.61
			128	Existing Control: Design - Where certain emails are blocked, the end-user will receive a Non-Delivery Report.	Accenture	Non Delivery Reports (NDRs)	v4.61
			129	Existing Control: Business Process Change - Emails that are flagged to the NHSmail Service Desk as having been incorrectly quarantined will be escalated to Trend Micro, and if indicated, added to the Trend pattern file.	Accenture	Reporting a false positive issue in Deep Security	v4.61

Hazard Event: Legitimate emails and attachments are quarantined and/or deleted (false positive).

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
66	Technical - False positives: The email Gateway security filters blocks or delays the exchange of legitimate email (false positive).	**v4.63**	127	Additional Control: Business Process Change - When sending important and time-critical information, end-users have a duty of care to ensure that its safe receipt is acknowledged. If receipt confirmation is not received then users should ensure that they make contact with the recipient and should never assume receipt.	Local Organisation		v4.61
			126	Additional Control: Business Process Change - Local organisations should have a support desk function to enable end-users to report mail flow issues, e.g. false positives. This should include an escalation process to the NHSmail helpdesk.	Local Organisation		v4.61
84	Technical - Business rule configuration: Clinical information sent as spoof mail is deleted by the email Gateway service. The sender may be unaware of this, believing that the mail has been received.	**v4.62**	890	Additional Control: Business Process Change - Local policy should align with the NHSmail Acceptable Use Policy with regards to spoofing and only include approved methods, such as delegation controls and impersonation accounts (individuals impersonated must always be informed before emails are sent).	Local Organisation		v4.63
			178	Existing Control: Design - The business rules that manage the spoofing of nhs.net include an exception rule to allow the forwarding of email from an NHS users legacy email account so that legitimate emails are not diverted to the recipients' junk folder following migration to NHSmail.	Accenture		v4.65.5
			512	Additional Control: Training - Guidance is provided on anti-spoofing.	NHS England	Anti Spoofing Controls	v4.65.5
			134	Additional Control: Business Process Change - End-users should regularly check their Junk mail folder, including any shared mailboxes they access, to ensure that no emails have been incorrectly diverted (only applies to organisations migrating to nhs.net).	Local Organisation		v4.58
			336	Existing Control: Business Process Change - Proactive monitoring of the Gateway service will identify when the deny list is used and ensure that, where indicated, de-listing is actioned promptly. (the de-listing process is dependent on third party organisations' process and can take several hours for the process to complete).	Trend Micro	Deny-Listing – Email sent to external recipients (e.g. Gmail / Hotmail / Outlook.com) may be blocked or delivered to junk	v4.61
			337	Additional Control: Business Process Change - Local organisations should maintain a record all applications that depend on the NHSmail service to send and receive emails via the Internet. This should include the business impact of delivery/receipt failure and the contingency measures to be used for each system.	Local Organisation	Contact NHSmail Service Desk	v4.61

Hazard Event: Legitimate emails and attachments are quarantined and/or deleted (false positive).

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
84	Technical - Business rule configuration: Clinical information sent as spoof mail is deleted by the email Gateway service. The sender may be unaware of this, believing that the mail has been received.	**v4.62**	177	Additional Control: Training - Guidance is provided on the configuring Application accounts and the correct protocol configuration to be used.	NHS England	Applications Guide	v4.63
			136	Additional Control: Business Process Change - NHSmail Acceptable Use Policy, which all users have to accept before using the NHSmail service, forbids the use of spoofing.	NHS England	NHSmail Acceptable Use Policy	v4.65.6
			889	Existing Control: Business Process Change - The security improvements around the blocking of all emails spoofing @nhs.net from the NHSmail service have been communicated to local organisations.	NHS England	Spoofing Email Block	v4.63
			175	Additional Control: Business Process Change - The business rules governing what happens to spoof email have been communicated to all NHSmail users, including, organisation administrators, end-users, senior stakeholders, e.g. CIO/CCIO network, as well as external organisations.	NHS England	Spoofing Recipient Email Removal	v4.61
			414	Additional Control: Business Process Change - When using email forwarding, for example, when migrating from a legacy email system to the NHSmail O365 Shared Tenant, the local organisation IP addresses should be added to the local exchange to prevent these emails from being incorrectly identified as spoof.	Local Organisation		v4.61
			809	Additional Control: Training - Guidance is provided on Mail management.	NHS England	Junk Mail Guidance Update	v4.65.2
150	Technical - Business rule configuration : Conditional mail routing fails due to erroneous or missing configuration.	**v4.61**	307	Additional Control: Testing - The business subject line and menu classification rules used for the conditional mail routing for inbound and outbound email traffic will be tested post-implementation to ensure that they conform to the approved configuration and intended workflow.	Accenture		v4.61
			308	Existing Control: Business Process Change - Configuration of all business rules will follow a structured change control process, including Senior Management approval (Accenture and NHS England).	Accenture		v4.61

Hazard Event: Legitimate emails and attachments are quarantined and/or deleted (false positive).

Application/Service Email Gateway (Relay)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
227	Technical - Silent removal of email attachments: Local Organisations may apply additional attachment blocking policies on their local email systems that may silently remove email attachments (this only applies to the *.nhs.uk domain). Encrypted attachments sent from nhs.net to secure domains are also typically removed.	**v4.63**	614	Additional Control: Training - Guidance is provided on the file attachment blocking practices that an organisation's endpoint security may use.	NHS England	Attachments Guide for NHSmail	v4.63

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
140	Human Factor - End-user awareness: End-user does not request an email delivery or read receipt.	**v4.61**	288	Additional Control: Training - Guidance is provided on how to use the email read and delivery receipts and any limitations.	NHS England	Requesting a read or delivery receipt	v4.61

Application/Service Microsoft Safe Links/ Safe Attachments

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
335	Technical - False positive: An email containing a URL or file attachment has been incorrectly blocked and quarantined, preventing the user from accessing legitimate content. (Note: this applies to external to nhs.net and nhs.net to nhs.net).	**v4.73.3**	1000	Additional Control: Business Process Change - If a false positive is identified, Microsoft can update their pattern file to reclassify the URL/attachment as safe and prevent future blocking (Note: this is a third party dependency with no defined SLA for this activity).	Microsoft		v4.73.1
			1042	Additional Control: Training - Help-site documentation on the Safe Attachments functionality will be made available to end-users to make them aware of how to review quarantined emails and report possible false positives.	NHS England	Safe Attachments	v4.73.1
			1032	Existing Control: Design - End-Users will receive a daily blocked attachments report, enabling them to review any blocked content. (Note: this will not include blocked URLs). Users can also check for quarantined emails at any time by accessing the Microsoft Security Centre directly at https://security.microsoft.com/ and logging in using their NHSmail credentials.	Local Organisation	How Safe Attachments works	v4.73.13
			1001	Additional Control: Business Process Change - The Safe Links/Attachments functionality will be implemented using a staged rollout to monitor false positive rates and to test the end-to-end processes, e.g. service design process.	NHS England		v4.73.1

Hazard Event: Legitimate emails and attachments are quarantined and/or deleted (false positive).

Application/Service Microsoft Safe Links/ Safe Attachments

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
335	Technical - False positive: An email containing a URL or file attachment has been incorrectly blocked and quarantined, preventing the user from accessing legitimate content. (Note: this applies to external to nhs.net and nhs.net to nhs.net).	v4.73.3	1006	Additional Control: Business Process Change - A user can request for a quarantined file or blocked URL to be made available via the Helpdesk if they suspect it is a false positive detection. Upon receiving such a request, the Helpdesk will contact Microsoft to investigate the file or URL. This process will determine if the file is safe to release and if the URL is safe to visit; this will lead to Microsoft updating its algorithms to prevent future false positives. Note: The email will be held in the Microsoft Security Centre for 30 days before it is automatically deleted.	NHS England		v4.73.3
			1005	Additional Control: Training - Help-site documentation on the Safe Links functionality will be made available to end-users to make them aware of how to review a blocked web address and report possible false positives.	NHS England	Safe Links	v4.73.1

HAZARD ID: H14 HAZARD: NHS directory contains incorrect, missing, or duplicate entries

V4.82

Hazard Event: NHS Directory contains incorrect, missing or duplicate entries.

Key Hazard Assumptions 1.The Local Administrator can login to their account.2. The Portal can be accessed.

Linked Hazards: H7:Unable to access NHSMail account; H10:Unable to administer user accounts

Context: The NHS Directory is available to all end-users. It holds the contact details, such as name, organisation, role and email address of all nhs.net and federated users. It is updated manually and through automated processes.

Hazard Event: NHS Directory contains incorrect, missing or duplicate entries.

Cause/s: See possible caues below

Effect: Difficulty in finding accurate contact information, delays or errors in referrals or consultations, compromised care coordination, misinformation or miscommunication, potential breach of patient privacy, increased risk of medical errors or delays in care.

Harm: Compromising care coordination and increasing the risk of misinformation or miscommunication. This can result in potential breaches of patient privacy and confidentiality, as well as an increased risk of medical errors or delays in care. Indirectly, this can negatively impact patient outcomes, hinder timely access to necessary healthcare services, and undermine the overall quality and safety of patient care.

Service/s: Microsoft Office 365 Online (SaaS) **Application/s:** Exchange Online; Outlook On The Web **Subservice/s:** Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Data Integrity **Hazard Status:** Open **Status Comment:** **Hazard Updated:** v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Low **Initial Clinical Risk:** 2 - Low

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Azure Active Directory

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
63	Technical - AD interface failure/performance: Failure of one or more AD interfaces (TANSync, ESR, NHSmail API) preventing the completion of the JML and/or reference data update processes. This may result in incorrect or incomplete end-user contact details.	v4.62	538	Additional Control: Testing - Local organisations should test TANSync as part of the onboarding process, and this should be repeated following any configuration changes.	Local Organisation	Joiner, Mover and Leaver (JML)	v4.62
			539	Additional Control: Training - Guidance is provided on JML Onboarding, including the end-to-end process in implementing the product, installing TANSync 2.0 and enabling Electronic Staff Record (ESR) Integration.	NHS England	Joiner, Mover and Leaver (JML)	v4.62
			540	Additional Control: Testing - The Identity Automation service interfaces have been tested to ensure that the configured JML data elements are synchronised following the approved design, and a 100% pass rate was achieved. A pilot of TANSync 2.0 and ESR to NHSmail integration was undertaken with select NHS organisations, and these components were found to be technically stable.	Accenture		v4.65.5
			575	Existing Control: Design - On receipt of the NHSmail inbound file, ESR will produce an outbound confirmation file which will detail the success of the email updates processed within ESR. There is also a retry process, which will attempt to reload the qualifying failed updates automatically.	Accenture		v4.65.5

Hazard Event: NHS Directory contains incorrect, missing or duplicate entries.

Application/Service Azure Active Directory

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
63	Technical - AD interface failure/performance: Failure of one or more AD interfaces (TANSync, ESR, NHSmail API) preventing the completion of the JML and/or reference data update processes. This may result in incorrect or incomplete end-user contact details.	**v4.62**	576	Existing Control: Design - An ESR /NHSmail O365 Shared Tenant /Local AD, JML comparison report, is available to Local Administrators to highlight any differences between the directory instances to aid identity matching.	Local Organisation	Admin Reports	v4.64
			536	Additional Control: Business Process Change - Notifications of scheduled ESR downtime are issued via a mailing list maintained by the NHS ESR Central Team and posted on the NHSMail Portal help pages.	NHS England	Announcements	v4.62
			537	Additional Control: Testing - Integration testing has been undertaken on each AD interface to identify any defects causing errors and timeouts and ensure that the traffic volume assumptions are valid. The end-user objects can be processed promptly and displayed within the AD user interface as expected.	Accenture		v4.65.5

Application/Service Electronic Staffing Record (ESR) Interface

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
104	Technical - End-user matching: ESR/NHSmail probability matching logic produces incorrect matches.	**v4.57**	579	Additional Control: Training - Guidance is provided on JML onboarding, including data validation, FAQ and onboarding support in resolve troubleshooting issues.	NHS England	Joiner, Mover and Leaver (JML)	v4.64
			574	Additional Control: Business Process Change - Local organisations are required to undertake a data validation exercise as part of the onboarding process. This will flag any employees that do not match cross the 3 platforms (Local org, NHSmail O365 Shared Tenant, ESR) using a set of key attributes, including first and last name, phone number and email address. This will ensure that those employees that need to be manually matched are identified. The data validation requires local organisations to provide sign-off as part of onboarding process and prior to cutover.	Local Organisation		v4.65.5
			578	Existing Control: Business Process Change - TanSync user record changes can be viewed in read-only mode by exporting to .xml format before synchronising end-user updates.	Local Organisation	TANSYnc Deployment Guide	v4.64
			206	Existing Control: Design - A duplicate user report is available for the local remediation of duplicate user accounts.	Local Organisation	Admin Reports	v4.57

Hazard Event: NHS Directory contains incorrect, missing or duplicate entries.

Application/Service Electronic Staffing Record (ESR) Interface

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
104	Technical - End-user matching: ESR/NHSmail probability matching logic produces incorrect matches.	**v4.57**	580	Additional Control: Design - Several reports are available to Local Administrators to support JML management, including a Mover Leaver Report – Lists all accounts (Users, Shared Mailboxes, Distribution Lists, Resource Mailboxes and Contacts) which joined, left the organisation or were transferred in the past 12 months, and a Contact Reports – Lists the details of all the contacts within the selected organisation, including the information visible on the Portal Admin pages as well as the contact's Local ID.	Local Organisation	Admin Reports	v4.64
			209	Additional Control: Training - Guidance is provided on TanSync, including the technical requirements and local organisation responsibilities for ensuring that all identities are matched correctly between the NHSmail Portal and local Active Directory before enabling the service.	NHS England	TANSync Guidance	v4.57
			207	Existing Control: Design - Matching will be done using a probability match based on a scoring system, which can be manually matched if the threshold is not reached.	Accenture		v4.65.5

Application/Service NHSmail Directory

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
81	Business Process - Contact management: Accounts are present in the NHS Directory when in a disabled state.	**v4.63**	171	Existing Control: Business Process Change - When a Local Administrator disables a user in the Portal they should check the directory to ensure that the user has been removed.	Local Organisation	Enabling and disabling a user account	v4.61

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
7	Business Process - Organisation and Sites Updates to Portal failure/error: Organisation and Sites Updates to the Portal Organisation Directory Service (ODS) is undertaken monthly as part of the standard change process. If this fails, updates to end-user directory objects will not be applied, and erroneous ODS data could overwrite correct portal entries.	**v4.63**	57	Additional Control: Business Process Change - A backup of the organisation/site information is taken and saved to a separate table to recover the original data if any error occurs.	Accenture		v4.61
			22	Existing Control: Testing - Post-implementation testing will verify the completion of the ODS export, i.e., the values of changed attributes match the ODS's Data. Spot checks post-implementation are also undertaken to verify that the exports have completed using the generated log files.	Accenture		v4.61

Hazard Event: NHS Directory contains incorrect, missing or duplicate entries.

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
7	Business Process - Organisation and Sites Updates to Portal failure/error: Organisation and Sites Updates to the Portal Organisation Directory Service (ODS) is undertaken monthly as part of the standard change process. If this fails, updates to end-user directory objects will not be applied, and erroneous ODS data could overwrite correct portal entries.	**v4.63**	55	Additional Control: Business Process Change - If the user data is incorrect, the Local Administrator can manually edit the entry in the Portal and also ensure that the ODS service has the correct user details so that the subsequent bulk upload applies the latest updates.	Local Organisation	Organisational attributes	v4.61
98	Human Factor - Manual update error: Local Administrator error in performing a manual update of the end-user contact details, e.g. name change.	**v4.57**	599	Additional Control: Design - The Local Administration Portal has been configured to use mandated entry fields to ensure that essential information is captured. Missing information will produce an error message under each missing field. Fields need to be completed before the user can be created.	Accenture	Creating and editing a contact	v4.63
			594	Existing Control: Design - When editing an NHS Directory Contact, changes are automatically updated on the NHS Directory and will apply to any distribution lists associated with the contact. The Portal displays success and failure notifications when edits are saved.	Accenture	Editing a NHS Directory contact	v4.62
			200	Additional Control: Training - Guidance is provided on how email aliases are managed. e.g. if a user gets married.	NHS England	Email Alias	v4.63
188	Business Process - Organisation Data Service (ODS)/NHSmail Portal data discrepancies: ODS updates are not applied or are applied with incorrect organisation contact details.	**v4.61**	425	Existing Control: Design - ODS updates are applied daily using a programmatic interface (the XML feed), ensuring that any updates made by the ODS team will be reflected within the NHSmail Directory almost instantaneously.	Accenture	Organisation Data Service (ODS) data feed	v4.61
			427	Additional Control: Business Process Change - Local organisations can raise ODS discrepancies with the ODS team (exeter.help-desk@nhs.net) and check whether an ODS code is active or closed using the ODS Portal search function.	Local Organisation	Organisation Data Service Portal	v4.65.2
189	Human Factor - Bulk Deletion of Portal Contacts: Directory contacts are erroneously deleted from the NHSmail Directory	**v4.61**	895	Existing Control: Design - A MailTip will notify the sender when a recipient is either not valid or no longer exists on NHSmail.	Microsoft	MailTips	v4.65.4
			430	Existing Control: Business Process Change - A back-up of all the contacts is taken as part of the implementation process, and a rollback can be performed, e.g. if bulk contacts are deleted in error.	Accenture		v4.61

Hazard Event: NHS Directory contains incorrect, missing or duplicate entries.

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
189	Human Factor - Bulk Deletion of Portal Contacts: Directory contacts are erroneously deleted from the NHSmail Directory	**v4.61**	428	Existing Control: Testing - The business rules used to identify inactive contacts marked for deletion are tested before implementation for errors. (Rule: contact belongs to an organisation that is now closed, or the contact is marked as a leaver and the contact hasn't been sent an email (from a nhs.net address) in the last 30 days).	Accenture		v4.65.5
			429	Additional Control: Business Process Change - Local organisations will be informed before the mailbox deletion of the actions required of end-users to retain their account. For example, log into their NHSmail account immediately and ensure that a log is performed at least every 90 days to keep the account active.	Accenture		v4.65.5
226	Technical - Push connector validation: Failure in the bulk upload of end-user contact details, e.g. CSV extract validation failure.	**v4.62**	597	Additional Control: Training - Guidance is provided on the NHSmail Push Connector, including how to submit the Push Connector data, use the CSV Upload Account Management (Portal), and format the Push Connector data submission.	NHS England	Push Connector Guide	v4.62
			596	Additional Control: Design - The Local Administrator can use the CSV file upload validation tool to check that the CSV file meets the criteria for submission. Validation errors are usually due to formatting or syntax errors. The list of file validation results will indicate any errors on a line by line basis.	Local Organisation	Bulk uploading users via CSV files	v4.62

Application/Service Portal Administration; Managed Migrations

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
80	Business Process - Account activation: Accounts present in the NHS Directory from the point that an account is created regardless of end user activation (e.g. during migration to NHSmail or a BAU account provisioning process).	**v4.63**	170	Additional Control: Business Process Change - Local Administrators should use automatic replies on accounts that are not active to inform senders that the account is no longer being monitored.	Local Organisation	Setting automatic replies (Out of Office)	v4.61

Hazard Event: User does not maintain their calendar.

Key Hazard Assumptions

Linked Hazards: H12: Updating patient care records

Context: Together with the Bookings and Teams Apps, the Outlook calendar is a core component of the Virtual Visits service. Users can share their calendar with other users from within their organisations. Where approved, users can also share their calendar availability/activities with users from outside of their organisation via the calendar federation service.

Hazard Event: User does not maintain their calendar.

Cause/s: See possible caues below

Effect: Missed or double-booked appointments, scheduling conflicts, delays or cancellations in patient care, compromised care coordination, decreased efficiency in managing tasks or responsibilities

Harm: Missed or delayed appointments can have negative implications, including compromised care coordination, inefficiencies in patient care delivery, an increased risk of miscommunication or errors, and potential treatment delays or disruptions. These consequences can result in suboptimal healthcare outcomes, delays in necessary interventions, and potential adverse effects on patient well-being.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: Exchange Online; Outlook On The Web

Subservice/s:

Category: Record Keeping

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Low **Initial Clinical Risk:** 2 - Low

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Azure Active Directory Connect

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
106	Technical - Active Directory synchronisation: A synchronisation process error prevents the shared calendar from updating.	v4.63	214	Existing Control: Testing - Calendar sharing will test organisational relationships and sharing policies to ensure synchronisation success, and failure modes function as expected.	Accenture		v4.63

Application/Service Exchange Online; Outlook 2010

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
329	Technical - Legacy software: From 1st May 2022, users on MS Outlook 2010 will no longer be able to connect to MS Exchange Online (Outlook 2010, is no longer supported by Microsoft, e.g. security updates are no longer applied). This means that users using NHSmail and Outlook 2010 on a device, will not be able to connect and all emails from Exchange Online will not be delivered and calendars will not sync.	v4.69.2	975	Existing Control: Business Process Change - Users can continue to access the Outlook Web Application through their browser (portal.nhs.net) or Outlook mobile app.	Local Organisation		v4.69.2
			978	Existing Control: Business Process Change - In accordance with the Data Security and Protection toolkit (Data Security Standard 8) Local Organisations should ensure that they survey their IT inventory to understand which assets are approaching end of life. All legacy software should be risk assessed, and if appropriate, treated as unmanaged and untrusted.	Local Organisation	Data Security and Protection Toolkit	v4.69.2

HAZARD ID: H15 HAZARD: User does not maintain their calendar

Hazard Event: User does not maintain their calendar.

Application/Service Exchange Online; Outlook 2010

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
329	Technical - Legacy software: From 1st May 2022, users on MS Outlook 2010 will no longer be able to connect to MS Exchange Online (Outlook 2010, is no longer supported by Microsoft, e.g. security updates are no longer applied). This means that users using NHSmail and Outlook 2010 on a device, will not be able to connect and all emails from Exchange Online will not be delivered and calendars will not sync.	**v4.69.2**	979	Additional Control: Business Process Change - NHS England has identified the organisations using Outlook 2010 and is working with these to transition to a supported Outlook Client.	NHS England		v4.69.2
			976	Additional Control: Training - Guidance is provided on the end of life of Office 2010 (including Outlook). This includes direct end-user/LA comms, LA Bulletin and Portal Announcements.	NHS England	Office 2010 important end date reminder	v4.69.2
			974	Existing Control: Business Process Change - Local organisations have a responsibility to ensure that they are using software capable of supporting the latest security updates.	Local Organisation		v4.69.2

Application/Service Microsoft Outlook Calendar

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
105	Human Factor - Calendar updates: Calendar information is not updated by the user, which, if used to schedule clinical activity, e.g. virtual consultations, may result in appointments having to be subsequently rescheduled.	**v4.63**	592	Existing Control: Business Process Change - End-users should block out calendar slots where they are unavailable and use the out-of-office function to ensure that senders are made aware of periods of absence. This is particularly important where appointments are scheduled into a user's calendar by another user, e.g. the Virtual Visits Bookings administrator.	Local Organisation		v4.64
			212	Additional Control: Business Process Change - Federation partners will be required to sign-up to a Federation Partnership Agreement acknowledging their obligations to ensure their users act following good practice and are sufficiently trained. The agreement should include the principle of ensuring clinical appointments are always captured in line with local policy and agreed standard operating procedures.	Local Organisation	NHSmail Acceptable Use Policy	v4.65.6
247	Human Factor - Appointment conflict: Appointment is double-booked into the calendar appointment slot causing a conflict and possible end-user confusion.	**v4.63.2**	666	Additional Control: Business Process Change - End-users should ensure that they maintain an up to date calendar by actively blocking out unavailable slots to ensure that free/busy periods are accurate. Slots booked in the Bookings app will automatically block out the user's availability in their calendar.	Local Organisation		v4.63.3

Hazard Event: User does not maintain their calendar.

Application/Service Microsoft Outlook Calendar

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
247	Human Factor - Appointment conflict: Appointment is double-booked into the calendar appointment slot causing a conflict and possible end-user confusion.	**v4.63.2**	770	Additional Control: Business Process Change - The organiser should select the 'Events on Office 365 calendar' setting to ensure that free/busy information from staff members' calendars is considered when determining their availability for an appointment.	Local Organisation	Virtual Visits – User Guidance	v4.64.2
			771	Additional Control: Business Process Change - Local organisations should define a process for confirming the availability of users who are unable to share their calendar, i.e. those not on Exchange Online.	Local Organisation		v4.64.2
			488	Additional Control: Design - All booked calendar slots are shaded for the duration of the appointment. After scheduling the appointment, the calendar booking screen is displayed, defaulting to the scheduled appointment date and time, making duplicate bookings apparent. Duplicate bookings can be cancelled and rebooked, and a free-text reason can be added to the cancellation, which will be included in the cancellation email.	Microsoft		v4.63.3
			436	Additional Control: Business Process Change - Where more than a single appointment booking system is being used, the local organisation should ensure that a process is in place to mitigate against the risk of omitted, duplicated or erroneously cancelled or rescheduled appointments.	Local Organisation		v4.63.2
262	Business Process - Calendar membership acceptance/rejection: The user is unaware that they have been added to a Bookings calendar.	**v4.63.3**	694	Additional Control: Training - Guidance is provided on calendar membership management.	NHS England	Virtual Visits – Local Administrator Guide	v4.63.3
			670	Additional Control: Business Process Change - Local organisations should have procedures to ensure that calendar membership acceptance/rejection is controlled to reduce the risk of acceptance delays and erroneous rejections.	Local Organisation		v4.63.3
			692	Additional Control: Design - When an end-user is added to a calendar by the Bookings administrator, they will receive an email to notify them. An 'important' action message will be displayed in red font, alerting the user that they must approve their membership. They are also warned of the consequence of stopping their membership, although they can resume it at any time.	Microsoft	Virtual Visits – User Guidance	v4.63.3

Hazard Event: User does not maintain their calendar.

Application/Service Microsoft Outlook Calendar

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
263	Technical - Appointment confirmation response misalignment: When an appointment is scheduled in the Bookings app, it will immediately synchronise with the user's Outlook and Teams Calendars. The user can then accept, reject or tentatively accept, but these responses only apply to the user's calendar, and not the original booking, e.g. a declined appointment will remain active in the Bookings app.	**v4.63.3**	619	Additional Control: Training - Guidance is provided covering the different appointment responses and the impact of each.	NHS England	Virtual Visits – User Guidance	v4.63.3
			662	Additional Control: Business Process Change - Local organisations should have procedures to manage end-user appointment responses, ensuring that the Bookings calendar is updated as soon as an end-user rejects an appointment. Tentative acceptance also needs to be monitored so that there is no ambiguity in the appointment acceptance status.	Local Organisation		v4.63.3
			664	Existing Control: Business Process Change - When the end-user accepts, declines or tentatively accepts an appointment, an email notification is sent to the Bookings administrator. (the toggle switch is set to notify the Bookings administrator by default and should not be changed unless the user also has admin rights). The user can also use the RSVP free-text field to propose an alternative appointment slot.	Local Organisation		v4.63.3

HAZARD ID: H16 HAZARD: User data fails to fully migrate

V4.82

Hazard Event: User data fails to fully migrate

Key Hazard Assumptions 1.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.

Linked Hazards: H2:Disrupted communication and workflow due to NHSMail outage; H7:Unable to access NHSMail account; H20:User cannot access Microsoft O365 applications or features

Context: Accenture performs migration activities as part of routine maintenance, e.g., content migration between environments as part of decommissioning activities and the Managed Migration Service. Migration may also involve self-migration of content.Managed Migrations is an additional catalogue service to support local organisations wanting to move to the NHSmail O365 Shared Tenant. It supports: • On-premise mail to NHSmail 0365 • Local file shares to NHSmail Share Point • Local home drives to NHSmail OneDrive4Business • Local pst file migrations to NHSmail 0365 Archive

Hazard Event: User data fails to fully migrate

Cause/s: See possible caues below

Effect: Loss of critical user data, data inconsistencies between systems, data corruption or loss, disruption of workflows, potential breach of data security and privacy

Harm: Data migration issues can result in indirect patient harm through delays in accessing records, disrupted communication among healthcare providers, compromised data security and privacy, and potential errors in patient care. These consequences can impact patient safety, trust, and the overall quality of healthcare services provided.

Service/s: Migrations

Application/s: Exchange; Online (and PST); SharePoint; OneDrive; Teams

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS); Avanade Tooling, e.g. O365 Accelerate, MigWiz; and SharePoint Migration Manager.

Category: Data Integrity

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Low **Initial Clinical Risk:** 2 - Low

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service IT Operations

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
143	Technical - Sever unavailability: Source server is unavailable.	v4.61	299	Existing Control: Business Process Change - If a source server is unavailable, the migration team will reschedule the mailbox moves to the following day.	Accenture		v4.61
144	Technical - Uncontrolled change: Uncontrolled or unspecified changes have been made to the target / source environment.	v4.61	300	Existing Control: Business Process Change - A process has been defined to ensure changes to the Microsoft environment are communicated in advance to the migration team.	Accenture		v4.61
			301	Additional Control: Business Process Change - Communications will be provided to local organisations to inform the migration team of any changes to their local environment to assess any potential impacts on the scheduled migration.	Accenture		v4.61

Application/Service Managed Migrations

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
134	Technical - Migration account scheduling: Migration tooling software fails to complete the scheduled migration tasks.	v4.54	924	Additional Control: Business Process Change - Local organisations should use the output of the pilot testing to test and refine key organisational processes.	Local Organisation		v4.65.5

Hazard Event: User data fails to fully migrate

Application/Service Managed Migrations

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
134	Technical - Migration account scheduling: Migration tooling software fails to complete the scheduled migration tasks.	**v4.54**	276	Additional Control: Business Process Change - Fully managed migrations include beta testing and pilot testing of around 5%-10% of in-scope users, and reports will be run to show the mailbox migration status up to completion.	Accenture		v4.65.5
142	Human Factor - Mailbox permissions: Mailbox does not been given the correct permissions.	**v4.61**	298	Existing Control: Business Process Change - Pre-requisite checks will be made to ensure each mailbox has the appropriate permissions to enable the migration to progress.	Accenture		v4.61
145	Technical - Data corruption: Number of bad mail items exceeds the threshold.	**v4.61**	904	Additional Control: Business Process Change - Local organisations should have business continuity procedures in place in the even that the migration process failures impacts the provision of care.	Local Organisation		v4.65.2
			905	Additional Control: Business Process Change - Source data is backed up prior to commencement of the migration process and post migration data integrity checks will be undertaken.	Accenture		v4.65.2
			906	Additional Control: Training - The Managed Migration team will provide guidance and support to the local migration team so that all local dependencies are understood.	Accenture		v4.65.2
			303	Existing Control: Business Process Change - The bad item threshold can be increased up to 150 bad items to enable migration to progress as scheduled. Mailboxes that cannot be migrated using the automated migration tooling will be manually migrated through a PST export process, for example, where the volume of corrupt mailbox items exceeds the permitted threshold. If this fails, a new mailbox can be created and emails imported.	Accenture		v4.63
314	Data - Data validation: Invalid data is contained within the migration dataset CSV file.	**v4.65.5**	928	Additional Control: Business Process Change - A checklist will be used to validate the data contained in the CSV dataset, e.g. valid email addresses, blanks, duplicate data values, name length checks.	Accenture		v4.65.4
315	Human Factor - Data accuracy: The source mailboxes have been incorrectly matched/identified prior to the migration.	**v4.65.5**	926	Additional Control: Business Process Change - Users that have been missed or incorrectly matched will be migrated during the Mop-Up phase.	Accenture		v4.65.4

Hazard Event: User data fails to fully migrate

Application/Service Managed Migrations

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
315	Human Factor - Data accuracy: The source mailboxes have been incorrectly matched/identified prior to the migration.	**v4.65.5**	927	Additional Control: Business Process Change - Changes to the Active Directory will be frozen following the submission of the CSV mailbox migration dataset file to reduce the risk of mismatches and omissions.	Accenture		v4.65.4
			932	Additional Control: Business Process Change - The Local Organisation should have a service desk function to resolve end-user migration queries/incidents. This should include an escalation route to the local migration support team.	Local Organisation		v4.65.4
			925	Additional Control: Business Process Change - Local organisations are required to sign a NHSmail Migration Data Accuracy form confirming that all current users are matched correctly to their existing NHSmail account and al new users have been identified to ensure they are provisioned a new account through the migration process.	Local Organisation		v4.65.4
316	Technical - API/policy limitations: API limitations of the source system limit prevent specific items/settings from being migrated, e.g. acceptance status for meetings, dynamic distribution lists, and email flags.	**v4.65.5**	931	Additional Control: Business Process Change - Communications will be issued to end-users to make them aware of what actions they need to take to address any gaps in the migration process, e.g. profile update, assign email signature.	Accenture		v4.65.4
			929	Additional Control: Training - Guidance is provided on the items that will not be migrated.	Accenture		v4.65.4
320	Technical - Mail Exchange (MX) record configuration/mismatch error: MX record error resulting in legacy email being routed to an invalid account in exchange, e.g. configuration error during set-up, incorrect mapping of user domains.	**v4.65.6**	948	Additional Control: Testing - Local organisations should ensure that the user domain mappings are validated before submission and submitted in an approved format, e.g. CSV file.	Local Organisation		v4.65.6
			949	Additional Control: Testing - Following the implementation of the MX Record, the Local Organisation should perform testing and confirm to Accenture that the change has been completed successfully.	Local Organisation		v4.65.6
			947	Additional Control: Testing - If the MX Record script fails the change can be reverted.	Accenture		v4.65.6

Hazard Event: User data fails to fully migrate

Application/Service Power Platform

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
336	Business Process - Power App/Flow migration not completed: The end-user fails to complete the Power Apps/Power Automate Flows migration by the cutover date, e.g. the user is unaware of the change, is unable to complete self-migration tasks or fails to do so.	**v4.72.1**	1011	Additional Control: Business Process Change - If the Power Apps and Power Automate Flows have not been migrated by the cutover date, temporary access (24hrs) to the legacy environment can be granted (this will be authorised through a service request).	Accenture		v4.72.1
			1015	Additional Control: Business Process Change - Ongoing monitoring and status reporting have been undertaken throughout the migration process and used to issue targeted comms to content owners and Local Administrators.	Accenture		v4.72.2
			1016	Additional Control: Training - All guidance including guidance on Migrating Apps and Flows has been published to the NHSmail support site.	Accenture	Power Platform Guidance	v4.72.3
			1010	Additional Control: Business Process Change - Communications have been issued to end-users to make them aware of the actions they need to complete to migrate their Power App apps and Power Automate flows from the default environment into the dedicated organisation environments.	Local Organisation		v4.72.1
337	Technical - New environment cutover unsuccessful: Cutover to new UK Environment from old EU Environment is unsuccessful, e.g. configuration error, performance issue.	**v4.72.2**	1014	Additional Control: Business Process Change - If the migration fails, rollback procedures will be invoked, e.g. resetting the default to the EU (not the UK environment) and restoring the UI setting to pre-implementation.	Accenture		v4.72.2
			1012	Additional Control: Testing - Following the migration of the Power App apps and Power Automate flows, users should perform testing to confirm that the migration has worked successfully before the old default environment is decommissioned.	Local Organisation		v4.72.1
			1013	Additional Control: Testing - Cutover testing has been completed on the new UK environment to ensure that the change has been correctly implemented and that the migration activities can be completed.	Accenture		v4.72.2

HAZARD ID: H17 HAZARD: Accessing third-party (federated) applications

Hazard Event: Single sign on failure.

Key Hazard Assumptions 1.The user can login to their account.

Linked Hazards: H7:Unable to access NHSmail account

Context: Approved third-party applications can be federated with the NHSmail O365 Shared Tenant, removing the need for users to manage multiple passwords. Users can use their NHSmail login credentials (Single-Sign-On) to access the applications.

Hazard Event: Single sign on failure.

Cause/s: See possible caues below

Effect: Inability to access systems or applications, delays or disruptions in workflow, potential data breaches or unauthorised access to sensitive information, increased support requests for login assistance

Harm: The failure of single sign-on (SSO) can result in indirect harm by disrupting workflow by preventing healthcare professionals from accessing essential information and tools. This may result in indirect patient harm through reduced efficiency in healthcare processes and challenges in providing timely and effective treatment.

Service/s: Active Directory Federation Service

Application/s: Third-Party Applications

Subservice/s: Azure (IaaS)

Category: Access

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Low **Initial Clinical Risk:** 2 - Low

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Active Directory Federation Service

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
79	Technical - Changes to third-party configuration/infrastructure: Federated partner changes may impact on service availability, e.g. recent SSL certificate renewal results in failure to complete the trust certification process.	v4.63	169	Additional Control: Business Process Change - Under the terms of the Federation Partner Agreement, local organisations are required to give notice of any local configuration changes that may impact other federated partners.	Local Organisation		v4.63
			168	Existing Control: Business Process Change - All changes to the NHSmail ADFS service adhere to ITIL. All changes must be impact assessed and approved by senior management and all national changes are also approved by NHS England. Post-implementation testing is undertaken in an appropriate test environment and once changes are deployed they can be rolled back if failures or errors are encountered.	Accenture		v4.63
			679	Additional Control: Training - Guidance is provided on Third-Party and Single Sign-On Certificate Renewal.	NHS England	Third Party & Single Sign-On Certificate Renewal Guide	v4.63
			680	Existing Control: Business Process Change - Local organisations should have a help desk function to resolve SSO access issues. If the help desk cannot provide resolution, a service incident can be raised with the NHSmail help desk.	Local Organisation	Contact NHSmail Service Desk	v4.63
			677	Existing Control: Testing - When a new third-party SSO relationship is configured, this undergoes post-implementation testing to ensure that the application can be accessed.	Accenture		v4.63

HAZARD ID: H17 HAZARD: Accessing third-party (federated) applications

V4.82

Hazard Event: Single sign on failure.

Application/Service Active Directory Federation Service

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated

HAZARD ID: H18 HAZARD: The appointment scheduler is unavailable or inaccessible

Hazard Event: The appointment scheduler is unavailable or inaccessible.

Key Hazard Assumptions 1.The user can login to their account.2.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.3.The O365 Bookings App can be accessed.

Linked Hazards: H2:Disrupted communication and workflow due to NHSMail outage; H7:Unable to access NHSMail account; H20:User cannot access Microsoft O365 applications or features

Context: The appointment scheduler is used in the Virtual Visits service. Calendars are created for a service or team, and these are assigned to members. Appointments are booked, and end-users and patients are notified by email.

Hazard Event: The appointment scheduler is unavailable or inaccessible.

Cause/s: See possible caues below

Effect: Inability to schedule or manage appointments, delays or disruptions in patient care, missed or rescheduled appointments, compromised care coordination, decreased efficiency in appointment management

Harm: The unavailability or inaccessibility of an appointment scheduler can lead to indirect harm to patients. It can result in appointment scheduling issues, causing delays in obtaining necessary medical care and disrupting care coordination between healthcare providers. This can lead to fragmented care and potentially adverse health outcomes. Additionally, patients may experience increased stress and anxiety when they cannot schedule appointments.

Service/s: Microsoft Office 365 Online (SaaS) **Application/s:** Bookings **Subservice/s:** Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Scheduling **Hazard Status:** Open **Status Comment:** **Hazard Updated:** v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Microsoft Bookings

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
12	Business Process - Bookings permissions : The permissions do not enable end-users to undertake their role effectively.	v4.63.2	236	Existing Control: Testing - Testing is undertaken to validate the Bookings menus/functions correspond to the configured Portal permissions/admin role mappings.	Accenture		v4.63.2
			757	Additional Control: Training - Guidance is provided on the administration of the Virtual Visits service.	NHS England	Virtual Visits – Local Administrator Guide	v4.64.2
			293	Existing Control: Testing - The local organisation should undertake testing to verify the calendar configuration and anticipated workflow for each team member to ensure that they can access the allocated calendar and perform all actions expected for their role.	Local Organisation		v4.63.2
			519	Additional Control: Design - The Bookings app roles can be allocated to support local business process and clinical workflow, e.g. a clinician can be allocated an administrator role if they are required to manage their appointment schedules.	Local Organisation		v4.63.2
62	Technical - Bookings event triggers: The Bookings technical workflow uses Azure Functions event triggers to communicate with the Graph API to create/update the Bookings calendars. Errors/failure may occur if the code or event trigger is configured incorrectly.	v4.62	752	Additional Control: Business Process Change - Service Management can investigate the log files to help resolve Portal/Graph API exception requests.	Accenture	Microsoft Graph error responses and resource types	v4.63.2

Hazard Event: The appointment scheduler is unavailable or inaccessible.

Application/Service Microsoft Bookings

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
62	Technical - Bookings event triggers: The Bookings technical workflow uses Azure Functions event triggers to communicate with the Graph API to create/update the Bookings calendars. Errors/failure may occur if the code or event trigger is configured incorrectly.	**v4.62**	750	Existing Control: Design - Azure Functions utilises debugging validation tools to enable coding errors to be highlighted during the specification of the event triggers.	Microsoft	Strategies for testing your code in Azure Functions	v4.64.2
			749	Additional Control: Testing - The Azure Functions event workflow triggers will be tested to validate the business logic inputs and outputs, e.g. MS Graph API POST/PATCH/GET requests. Testing will also cover exceptions workflow, e.g. staff member has not been added to the calendar as the user account has not been migrated to Exchange Online. In such cases, the messaging workflow will notify the administrator by email.	Accenture		v4.64.2
			560	Existing Control: Design - The calendar bookings page will use validation rules to mandate essential data entry fields and prompt users to confirm important actions, e.g. when a calendar is deleted. A pop-up window will prompt the user to confirm the deletion action.	Accenture	Virtual Visits – Local Administrator Guide	v4.64.2
69	Human Factor - Calendar configuration: The Bookings team calendar has been incorrectly configured, or the correctly specified configuration does not enable the team to function effectively.	**v4.62**	559	Additional Control: Testing - Local organisations should perform post-implementation testing of calendar changes to ensure that they can be retrieved and to verify that the naming logic adheres to local policy.	Local Organisation		v4.64.2
			625	Additional Control: Design - The team Bookings calendar should be specified by the local team considering the type and range of patient appointments that will need to be scheduled by the team, including sufficient appointment slot length and users that may need to provide regular cover, such as bank staff.	Local Organisation		v4.64.2
			655	Additional Control: Business Process Change - A formal review and approval cycle should support the specification of the Team calendars to reduce the risk of errors being introduced into live service.	Local Organisation		v4.64.2
78	Human Factor - User not assigned/removed: The user has not been assigned to the team/service calendar that they are attempting to access, or they have been removed without notice.	**v4.62**	550	Existing Control: Design - The deletion of users from a calendar is restricted to those with Administrator permission rights: Bookings Admin, Local Admin; Local Primary Admin; Global Admin and Tenant Admin.	Microsoft	Virtual Visits – Local Administrator Guide	v4.64.2

Hazard Event: The appointment scheduler is unavailable or inaccessible.

Application/Service Microsoft Bookings

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
78	Human Factor - User not assigned/removed: The user has not been assigned to the team/service calendar that they are attempting to access, or they have been removed without notice.	**v4.62**	546	Existing Control: Design - When a user is removed from a calendar schedule, a pop-up window will prompt the Administrator to confirm the deletion action, reducing the likelihood of accidental removal.	Microsoft	Virtual Visits – Local Administrator Guide	v4.64.2
			551	Additional Control: Design - If a user is removed from a calendar schedule, they will continue to have access to all booked appointments in their Outlook calendar. If a user is mistakenly removed, they can be reinstated.	Microsoft		v4.64.2
244	Technical - Bookings app unavailable: The app is unavailable, which may prevent new appointments being scheduled or existing appointments from being viewed or amended.	**v4.63.2**	518	Additional Control: Design - If the Bookings app is unavailable, end-users should be able to access existing appointments using the Outlook calendar.	Local Organisation		v4.63.2
			420	Additional Control: Business Process Change - Local organisations should ensure that the Business Continuity and Disaster Recovery plan provides contingency if the Bookings app is unavailable, covering how existing and new appointment bookings will be managed.	Local Organisation		v4.63.2
			751	Additional Control: Design - The Local Administrator must enable the Bookings app in the User Policies, including when a user joins or transfers to another organisation that does not have the appropriate O365 licence/Portal user policy configuration.	Local Organisation	Virtual Visits – Local Administrator Guide	v4.63.2
245	Human Factor - Bookings calendar retrieval: The administrator is unable to locate or access the appointment calendar/s, e.g. calendar has been deleted.	**v4.63.2**	562	Existing Control: Design - The deletion of the calendar schedule can be restricted through configuration. Only users with the BOOKING_CALENDAR_DELETE permission can perform a deletion action, and any deletions can only be done against the user's registered organisation.	Accenture	Virtual Visits – Local Administrator Guide (Update or delete an existing Booking calendar)	v4.64.2
			60	Additional Control: Design - The calendar's name and email address are created automatically by combining the organisation's short name, followed by the service area and clinic name. This reduces the complexity and risk of user error in creating calendar schedules across multiple teams and services.	Accenture	Virtual Visits – Local Administrator Guide	v4.63.2
			74	Additional Control: Training - Guidance is provided on calendar naming convention.	NHS England	Virtual Visits – User Guidance	v4.64.2

Hazard Event: The appointment scheduler is unavailable or inaccessible.

Application/Service Microsoft Bookings

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
253	Technical - Appointment synchronisation failure: When an appointment is scheduled in the Bookings app, it should immediately synchronise with Outlook and Teams Calendars. Errors in the calendar sync process may result in the appointment not showing in the calendar.	**v4.63.2**	75	Existing Control: Testing - Local organisations should test any newly configured calendars to ensure that appointments made in the Bookings app populate the member calendars and that the appointment details match.	Local Organisation		v4.63.2
			714	Existing Control: Testing - Testing has been undertaken to verify that appointments scheduled or changed in the Bookings app are synchronised to the correct Outlook and Teams Calendars and align with the scheduled booking.	Accenture		v4.65.5
264	Technical - Booking confirmation: When scheduling an appointment using the Bookings app, no on-screen confirmation is presented to the user to indicate that an appointment has been successfully booked.	**v4.63.3**	667	Additional Control: Business Process Change - After scheduling an appointment, the administrator should verify the appointment details by checking the Bookings calendar screen.	Local Organisation		v4.63.3
			669	Existing Control: Design - The Bookings calendar screen automatically defaults to the date and time of the booked appointment, and hovering over the appointment slot will show the appointment details.	Local Organisation		v4.63.3

HAZARD ID: H19 HAZARD: Patient does not receive appointment invite

V4.82

Hazard Event: Patient does not receive appointment invite.

Key Hazard Assumptions 1.The user can login to their account.2.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.3.The O365 Bookings App can be accessed.

Linked Hazards: H2:Disrupted communication and workflow due to NHSmail outage; H7:Unable to access NHSmail account

Context: The appointment scheduler is used in the Virtual Visits service. Calendars are created for a service or team, and these are assigned to members. Appointments are booked, and end-users and patients are notified by email.

Hazard Event: Patient does not receive appointment invite.

Cause/s: See possible caues below

Effect: Patient not being aware of the appointment, missed or delayed attendance, potential gaps in patient care, reduced patient satisfaction, potential disruptions in care coordination.

Harm: Missed or delayed appointments can indirectly harm patients by disrupting care provision and creating gaps in patient care, potentially resulting in delays in diagnosis, treatment, or follow-up care.

Service/s: Microsoft Office 365 Online (SaaS) **Application/s:** Bookings **Subservice/s:** Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Scheduling **Hazard Status:** Open **Status Comment:** **Hazard Updated:** v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Low **Residual Clinical Risk:** 2 - Low

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
70	Human Factor - Invite acceptance: HCP does not confirm acceptance of the invite.	v4.62	761	Additional Control: Training - Guidance should be provided to users on what actions to take if they are unable to attend their scheduled appointment.	Local Organisation		v4.64.2
			738	Additional Control: Business Process Change - Local organisations should have procedures to support the effective management of patient appointments, including follow up. The procedures should include steps that the requestor has to follow, such as maximum time to notify the Bookings Administrator, read/delivery receipts when submitting a booking request by email and checking the Outlook calendar to confirm that the booking has done.	Local Organisation		v4.64.2
			709	Additional Control: Business Process Change - A process should be in place to manage tentative and declined appointments so that all attendees confirm the appointment status before the consultation date.	Local Organisation		v4.64.2
			502	Additional Control: Training - Guidance is provided on the use of the email reminder feature.	NHS England	Virtual Visits – User Guidance	v4.63.2
			419	Additional Control: Business Process Change - If an end-user does not receive an appointment reminder, they should check their junk mail folder. Emails that are diverted to the junk folder should be marked as 'not spam so that they are subsequently delivered to the user's inbox. If the patient does not receive their appointment email, they should contact the local organisation to ensure that the booking has been made.	Local Organisation		v4.63.2

Hazard Event: Patient does not receive appointment invite.

Application/Service Exchange Online; Outlook On The Web

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
70	Human Factor - Invite acceptance: HCP does not confirm acceptance of the invite.	**v4.62**	296	Additional Control: Design - The Bookings administrator can configure the appointment email reminder setting (15min to 3weeks), enabling an optimum window to be set for each calendar, dependent on local preference.	Local Organisation		v4.63.2
252	Human Factor - External users: Users that have not migrated to Exchange Online or persons that the patient wants to attend the consultation with will not receive an automated appointment email, reminder email or any subsequent workflow notification email following any changes to the scheduled booking.	**v4.63.2**	521	Additional Control: Training - Local organisations should provide guidance on inviting external users to participate in a consultation. This should cover appointment reminders and their limitations so that all users are aware that any edits made to an existing appointment will not automatically notify external users.	Local Organisation		v4.63.3
			653	Existing Control: Business Process Change - Email delivery and read receipts should be used when forwarding appointment invites to patients and additional users.	Local Organisation	Requesting a read or delivery receipt	v4.63.3
282	Human Factor - Email access: The patient may be unable to access their email account to retrieve the appointment email.	**v4.65.1**	732	Additional Control: Business Process Change - Local organisations should ensure that a process is in place for the follow up missed appointments.	Local Organisation		v4.64.2

Application/Service Microsoft Bookings

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
110	Human Factor - Email deletion: The user or patient may accidentally delete the appointment email.	**v4.62**	730	Existing Control: Design - Deleted emails can be recovered from the email deleted items folder.	Local Organisation	Opening and deleting emails	v4.64.2
111	Human Factor - Email address error: The Bookings Administrator may use an incorrect email address to send the appointment (Bookings does not use email read and delivery receipts).	**v4.62**	741	Existing Control: Design - Users on Exchange Online are selected from the directory with no requirement to enter an email address.	Microsoft	Using the NHS Directory (People Finder)	v4.64.2
			731	Additional Control: Design - The email address field within the Bookings application uses simple field validation to highlight email address input errors.	Microsoft		v4.64.2

Hazard Event: Patient does not receive appointment invite.

Application/Service Microsoft Bookings

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
176	Human Factor - User oversight: User/patient confirms acceptance but forgets to attend the consultation, particularly if the invite is received far in advance of the scheduled appointment.	**v4.62**	77	Additional Control: Business Process Change - Appointment reminders should be set, both for the patient and any end-user added to the invite (so long as they have an Exchange Online account). Reminder emails can be sent as soon as an appointment is booked, cancelled or rescheduled, and administrators should use them to reduce the risk of non-attendance.	Local Organisation	Virtual Visits – User Guidance	v4.63.2
215	Human Factor - Calendar membership: When the Administrator creates a bookings calendar, each user must accept the calendar invite to enable appointments to be scheduled in the calendar. The user can stop the calendar membership at any time; however, this will also prevent the scheduling of appointments.	**v4.62**	768	Additional Control: Design - When an end-user is added to a calendar by the Bookings administrator, they will receive an email to notify them. An important action message will be displayed in red font, alerting the user that they must approve their membership.	Microsoft	Virtual Visits – User Guidance	v4.64.2
			767	Additional Control: Business Process Change - Local organisations should have procedures in place to ensure that calendar membership acceptance is actively monitored, taking into consideration the joiner, mover and leaver processes, as well as unplanned absence.	Local Organisation		v4.64.2
			766	Additional Control: Business Process Change - The calendar membership process should ensure that end-users added to a calendar are aware to expect the calendar membership email (the calendar membership email process does not support automated reminders or read/delivery receipts).	Local Organisation		v4.64.2
			769	Additional Control: Training - Guidance is provided on calendar management.	NHS England	Virtual Visits – Local Administrator Guide	v4.64.2
229	Human Factor - Incorrect recipient selected: The user selects an incorrect patient when undertaking the appointment booking.	**v4.65.1**	760	Additional Control: Business Process Change - Users should check the appointment details before and after booking the appointment to ensure that the correct patient, team calendar, slot, HCP's etc., have been selected. Appointment verification is essential where multiple browser tabs have been opened to manage different team calendars.	Local Organisation		v4.64.2
240	Technical - Patient attendance: The email invite sent to patients does not allow the user to decline the invite and/or propose an alternative day/time.	**v4.62**	762	Additional Control: Business Process Change - The appointment invitation email should use the additional information section to communicate information about preparing for the virtual consultation and what to do if the appointment is unsuitable or if problems are experienced in completing the pre-requisite activities, e.g. unable to download software or network issues.	Local Organisation	Virtual Visits – User Guidance (local organisation processes)	v4.64.2

Hazard Event: Patient does not receive appointment invite.

Application/Service Microsoft Bookings

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
256	Technical - Appointment synchronisation failure: When an appointment is scheduled in the Bookings app, it should immediately synchronise with the Outlook and Teams Calendars. Errors in the calendar sync process may result in the appointment not showing in the calendar.	**v4.62**	735	Additional Control: Testing - The appointments bookings workflow functionality will be tested to verify that the appointment details display correctly in the target calendars.	Accenture		v4.65.5
257	Human Factor - User not assigned/removed: User unable to accept invite as they have not been assigned to the team/service calendar or they have been removed without notice.	**v4.65.1**	736	Additional Control: Business Process Change - Local organisations should ensure that procedures are in place for managing calendar membership.	Local Organisation		v4.64.2
281	Technical - Appointment not sent: The appointment may be created but the Bookings Administrator may fail to send it.	**v4.62**	443	Existing Control: Design - If the user exits the booking screen without submitting the appointment then an on-screen 'are you sure you want to leave' pop-up message will be displayed to the user.	Local Organisation		v4.63.2

HAZARD ID: H20 HAZARD: User cannot access Microsoft O365 applications or features

V4.82

Hazard Event: User cannot access Microsoft O365 applications or feature.

Key Hazard Assumptions 1.The user can login to their account.2.The NHSmail O365 Shared Tenant sub-services (Azure/AWS/MS Datacentres) are available.3.The app resides in the correct environment (for organisation/self-managed apps, e.g. Power Apps).

Linked Hazards: H2:Disrupted communication and workflow due to NHSmail outage

Context: Even when a user has successfully logged into their account, access to the O365/Azure applications or features is dependent on several factors, including licence allocation, user policy settings and AUP acceptance status. Note: A User account converted to an Application account is also subject to completing pre-requisite steps, e.g. AUP acceptance.

Hazard Event: User cannot access Microsoft O365 applications or feature.

Cause/s: See possible caues below

Effect: Inability to access O365 applications or features, delays or disruptions in work tasks, reduced productivity and efficiency, potential data loss or inconsistencies, compromised collaboration and communication.

Harm: The inability to access Microsoft O365 applications or features can indirectly harm patients by causing missed treatments, delayed care, compromised clinical decision-making, disrupted care coordination, communication breakdowns, and reduced efficiency in patient management.

Service/s: Microsoft Office 365 Online (SaaS)

Application/s: O365 Applications e.g. Exchange Online; Outlook On The Web; Teams; SharePoint; OneDrive; Azure relying party apps, e.g. Microsoft Defender for Endpoint.

Subservice/s: Azure (IaaS); Microsoft Datacentres (IaaS)

Category: Access

Hazard Status: Open

Status Comment:

Hazard Updated: v4.78.1

CLINICAL RISK ASSESSMENT

Initial Risk Assessment

Initial Severity: Considerable **Initial Likelihood:** Medium **Initial Clinical Risk:** 3 - Medium

Residual Risk Assessment

Residual Severity: Considerable **Residual likelihood:** Very Low **Residual Clinical Risk:** 2 - Low

Application/Service Bring Your Own Device (BYOD)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
347	Business Process - Policy restrictions: BYOD Conditional Access policies can restrict certain features, e.g. preventing downloading and printing of attachments when accessing O365 apps via a Web browser from an untrusted location (non-HSCN connection). Note: BYOD policy configuration is subject to the user licence type.	V4.76.1	1050	Additional Control: Business Process Change - If unanticipated restrictions on clinical user workflow are encountered, the Local Administrator can raise a service request to change the user's security group membership.	Accenture		v4.76.1
			1049	Additional Control: Training - The NHSmail Portal help pages include BYOD onboarding guidance.	NHS England	Bring Your Own Device Security Controls | Overview	v4.76.1
			1048	Existing Control: Business Process Change - BYOD policy restrictions will be bypassed when accessing the O365 applications from a Trusted Location (HSCN). If the organisation does not use the HSCN, a request can be submitted for specific IP addresses to be added to an 'allow list'. Note: IP requests will require a live service and security review and will approved on a case-by-case basis.	Accenture		v4.76.1

Hazard Event: User cannot access Microsoft O365 applications or feature.

Application/Service Exchange Online

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
345	Technical - Basic authentication deprecation: Microsoft will deprecate several Basic authentication protocols in 2023 to boost security and promote modern authentication. On April 27, EAS and RPC over HTTP will be deprecated, followed by EWS, POP, IMAP, and RPS on May 25. Consequently, mobile apps and desktop clients using Basic authentication will be unable to connect to Exchange Online to send or receive email.	**V4.77.1**	1053	Additional Control: Business Process Change - Local Administrators and end-users should follow the guidance on the NHSmail portal help pages to ensure service continuity. Outlook on the Web and the Outlook Mobile App, which utilise Modern Authentication, will continue to provide secure access to email, calendar, and contacts.	Local Organisation	Basic authentication deprecation	v4.77.1
			1054	Additional Control: Business Process Change - The deprecation process of Exchange Active Sync (EAS), will be staggered over 4 days to allow for proactive monitoring and mitigation of any issues that may arise, reducing the risk of adverse impacts on end-users.	Accenture		v4.77.1
			1043	Additional Control: Training - The deprecation of the Basic Authentication protocol has been communicated on the NHSmail Portal Announcements/help pages, LA bulletin and by email to end-users and Local Administrators.	NHS England	Local Administrator (LA) bulletin – 31 March 2023	4.77.1

Application/Service Intune

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
332	Technical - Mobile Application Management (MAM) Policy: If a locally configured Mobile Application Management (MAM) policy is too restrictive, user access to legitimate applications or features could be blocked.	**V4.70.1**	991	Additional Control: Testing - Local Administrators should validate all locally defined MAM policies to confirm that the targeted app exhibits the behaviour applied in the app configuration policy.	Local Organisation		V4.70.1
			987	Additional Control: Design - The NHSmail service has configured a standardised set of MAM policies that organisations can select from to reduce the risk of user set-up error.	NHS England	NHSmail Intune	V4.70.1

Application/Service Microsoft Office 365 Online (SaaS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
270	Technical - User Policy configuration: The O365 application toggle control has not been enabled in the User Policy Management settings.	**V4.70.1**	718	Existing Control: Design - The core O365 applications, e.g. Teams, SharePoint and OneDrive, are enabled by default to all NHSmail users as part of the NHSmail NHSE/MS national licensing agreement (N365). The Local Administrator can control the toggle switch in User Policy Management.	Local Organisation	User Policy Management: Editing a policy	v4.70.1

Hazard Event: User cannot access Microsoft O365 applications or feature.

Application/Service Microsoft Office 365 Online (SaaS): Azure Active Directory

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
330	Business Process - AUP not accepted: Users who do not accept the NHSmail Acceptable Use Policy (AUP) will be unable to access O365 and Azure AD applications, including Exchange Online, OWA, Teams, Office Suite and MS Defender for Endpoint. This restriction also applies to User accounts that have been converted to Application accounts, in addition to Service accounts.	**V4.70.1**	983	Additional Control: Training - Guidance is provided through LA Comms, Support Site Announcements and End User Comms on the importance of accepting the AUP and how to do so.	NHS England	Acceptable Use Policy	V4.70.1
			982	Additional Control: Training - Before AUP acceptance becomes compulsory, all end-users will receive a reminder, "You must accept the NHSmail Acceptable Use Policy (AUP) to access the NHSmail shared tenant services". This message will be displayed on the NHSmail Portal Login screen	NHS England		V4.70.1
			984	Additional Control: Business Process Change - Metrics monitoring will be conducted to ensure the work being carried out (Comms, Portal Reminder Message, update to AUP policy) is having a positive impact on the number of users accepting AUP.	Accenture		V4.70.1
			985	Additional Control: Design - End-users that have not accepted the AUP in the NHSmail Portal will encounter an error message when trying to access O365/Azure AD applications and be provided explicit instructions on what actions they must take to resolve.	Accenture		V4.70.1
331	Technical - AUP acceptance processing delay: When a user accepts the AUP, a backend process is run to update the NoAUP security group, which should take a few seconds. The processing time, however, may be extended where high volumes of users accept the AUP simultaneously or Portal performance issues are encountered.	**V4.70.1**	986	Additional Control: Business Process Change - If following AUP acceptance, the user cannot access the O365/Azure applications, a service request can be raised to manually remove the user from the NoAUP security group.	Accenture		V4.70.1

Application/Service NHSmail O365 Shared Tenant

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
112	Technical - Licence expiry: O365 licence assigned to the users NHSmail account has expired.	**v4.70.1**	224	Existing Control: Business Process Change - Local Administrators will be notified by email before the expiry of the O365 licence.	Microsoft		v4.70.1

Hazard Event: User cannot access Microsoft O365 applications or feature.

Application/Service Portal Administration

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
280	Business Process - O365 licence assignment: The O365 licence (or correct licence) has not been assigned to the users NHSmail account, has expired or been removed by the Local Administrator.	**V4.70.1**	723	Existing Control: Design - Local Administrators will have access to an O365 licensing report, which will include the expiry date for all end-user licences. Organisations using non-national licences will be able to produce a report of the licence information for their O365 subscriptions, which will include expiry details for all allocated licence	Local Organisation	Admin Reports	v4.70.1
			722	Existing Control: Business Process Change - Local Administrators will be notified by email before the expiry of the O365 licence.	Microsoft		v4.70.1
			721	Additional Control: Design - Users will automatically be added into their organisation's national policy, which utilises the nationally provided E3R licence (default licence type).	NHS England	NHSmail Office 365 Licence Matrix	v4.70.1
			988	Additional Control: Business Process Change - When a user is onboarded to a new organisation, the Local Administrator should ensure that the correct licence type is allocated to their account to enable the user to perform the tasks expected of their role. This may include 'add-on' and/or 'top-up' licence types.	Local Organisation	NHSmail Office 365 Licence Matrix	V4.70.1

Application/Service Security Groups

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
351	Business Process - O365 user licence migration: The transition from the current national license to a new license type and the shift from Direct licensing to Group-Based licensing may result in service disruption.	**v4.81.1**	1066	Existing Control: Business Process Change - User policies have been mapped to new license types and security groups, following a 1:1 mapping from previous configurations. This preserves existing policies, ensuring a near seamless transition.	NHS England		v4.81.1
			1067	Existing Control: Business Process Change - The migration will be executed in a phased approach to contain any technical issues, thus minimising potential adverse effects on end users.	Accenture		v4.81.1
			1068	Existing Control: Business Process Change - Verification will be undertaken to ensure the accurate assignment of user licenses and to correct licensing errors within groups. This will be done before the direct license is removed.	Accenture		v4.81.1
			1069	Additional Control: Business Process Change -			

Hazard Event: User cannot access Microsoft O365 applications or feature.

Application/Service Transport Layer Security (TLS)

ID	Possible Causes	Last Updated	ID	Controls and Mitigations	Owner	Reference	Last Updated
344	Technical - TLS version deprecation: The NHSmail Tenant no longer supports TLS 1.0 and 1.1 authentication requests. Organisations that do not upgrade to TLS 1.2 will be unable to connect to O365/AAD.	**v4.73**	1039	Existing Control: Business Process Change - Rollback procedures can be invoked if there is a clinical impact. Important: rollback can take around 1 hour and will not be available at all after 31st October 2022. All rollback requests must be approved by NHSE.	Accenture		v4.73
			1040	Additional Control: Business Process Change - NHSE have identified all accounts using TLS 1.0 and 1.1 and have been using this data to target affected users and organisations directly to update to v1.2.	NHS England		v4.73
			1041	Additional Control: Business Process Change - The TLS change has been communicated to Local Administrators via the LA Bulletin and LA Webinar. Direct comms have also been sent to users that will be impacted by the change.	NHS England	Recorded LA webinar sessions - 12th August 2022	v4.73
			1038	Additional Control: Training - Guidance is provided on the impact of the TLS deprecation and what actions organisations need to take to enable TLSv1.2.	NHS England	Transport Layer Security (TLS) Deprecation Guidance	v4.73