NHSmail Office 365 Teams deployment

Information governance considerations

November 2020
Version 3

Contents

Introduction

This document outlines considerations for local IT and IG departments in relation to the local implementation of the Microsoft NHSmail Office 365 (O365) collaboration capabilities from an information governance (IG) perspective for users in England. The primary focus in this document is Microsoft Teams.

It follows the process set out in the ICO's (Information Commissioner's Office) guidance for Data Protection Impact Assessments (DPIAs), and should be read alongside the guidance and criteria for an acceptable DPIA set out in European guidelines on DPIAs and a local organisation's IG policies and procedures.

The NHSmail DPIA is available on the NHSmail support site.

Microsoft guidance is also available: Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365

Step 1: The need for a DPIA

Users of the NHSmail service will create, store and send data through NHSmail and O365 services (including SharePoint, OneDrive, Teams) for collaboration purposes.

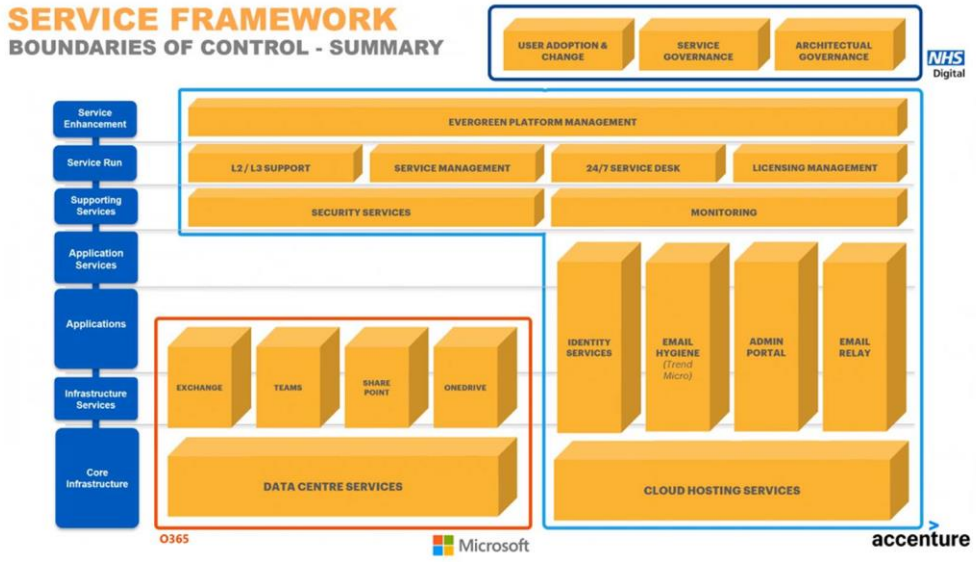
This data is controlled by the local organisation (as the joint controller with NHS Digital) and may include personal identifiable data and / or sensitive data. Local organisations are responsible for ensuring the data their users exchange has appropriate legal and governance controls in place, as well as completing a DPIA and publishing appropriate privacy information to patients.

Article 35 of the GDPR requires a data controller to create a DPIA "[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons."

Any local assessment should be made in conjunction with the published NHSmail DPIA and compliance with any existing local information governance policies.

Step 2: The processing of data

Data is processed in accordance with the Microsoft O365 service framework which is outlined below.



The below table outlines data category being processed by purpose, and type.

Category	**Who's information**	**System**	**Nature and purpose of the processing**	**Frequency** e.g. daily, weekly, monthly, real time	**Method of transport** Electronic system transfer, fax, secure email, paper or shared drive, post	**PID / No PID**	**Type of information** e.g. letter, report, referral or patient history
NHS Directory and metadata	Controller staff, controller service recipient	NHSmail and O365	Administration of services provided by NHSmail	Real-time	Electronic system transfer - EST	PID	Business identifiers - email address, - telephone number - organisation First name Last name
Content stored within NHSmail and O365 collaboration services i.e. Teams and OneNote	Controller staff, controller service recipient staff, NHS patients, member of the public	NHSmail and O365	Processing and storage of email and other data.	Real-time	Electronic system transfer - EST	PID	Patient identifiable data which may include reports, medical images, passport detail copies, financial data, other personal identifiers.

Data uploaded by users could include any aspect of local NHS business workflows and operations where there is a need to conduct cross working communication and collaboration - this includes the use of patient identifiable data which could be shared with NHS staff. Users of the service are required to comply with any existing local information governance policies

O365 data is stored by Microsoft. Depending on the specific service this may either be within the UK, EU or outside the EU and may be dependent on a local organisation's (joint controller) arrangements with Microsoft and the applications in use. For further information see Microsoft's privacy information.

Data is stored / processed by Microsoft by application, in the following locations as detailed in the published - Microsoft guidance on data locations.

Points to note:

- Applications above where data does not reside in the United Kingdom will be disabled by default by NHS Digital. If required, an organisation will need to enable these on a per user basis aligned to local policies.
- United Kingdom refers to data which is stored in either Durham, London, or Cardiff.
- The content, nature and length of time data is stored will be determined by an individual user's use of the provided collaborative functionality with reference to the published NHS data retention and information management policy for Office 365
- The Azure Active Directory data is processed in UK and USA data centres for resilience and availability.

Microsoft processing of user data

Microsoft, as a data processor, processes user data to provide online services in accordance with the customer's documented instructions. Microsoft also uses personal data to support a limited set of legitimate business operations internally.

Microsoft guidance is available: Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365.

Microsoft is the controller of the processing of personal data to support these specific legitimate business operations and aggregates personal data before using it for these purposes, removing Microsoft's ability to identify specific individuals.

Personal data is used in the least identifiable form that will support processing necessary for legitimate business operations. Microsoft will not use user data or information derived from it for profiling or for advertising or similar commercial purposes.

Microsoft responsibilities

Microsoft practises privacy by design and privacy by default in its engineering and business functions. As part of these efforts, Microsoft performs comprehensive privacy reviews on data processing operations that have the potential to cause impacts to the rights and freedoms of data subjects.

Privacy teams embedded in the service groups review the design and implementation of services to ensure that personal data is processed in a respectful manner in accordance with international law, user expectations and express commitments.

A number of detailed privacy reviews form a single DPIA that covers major groupings of processing, which the Microsoft EU Data Protection Officer (DPO) then reviews. The Microsoft EU DPO assesses the risks related to the data processing to ensure that sufficient mitigations are in place. If they find unmitigated risks, they will recommend changes back to the engineering group. DPIAs will be reviewed and updated as data protection risks change.

Microsoft guidance is available: Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365

Local organisations - processing and responsibilities

SharePoint, OneDrive and Office Online have been enabled for NHSmail users in order to facilitate the use of collaborative features in Teams. It is recommended that these applications are used in accordance with local information governance and clinical safety guidelines.

Note: SharePoint sites and Teams can only be set up and managed by Local Administrators (LAs). Guidance is available on how to find your Local Administrator.

Local organisations are responsible for ensuring the data their users store and exchange through the available capabilities are subject to the appropriate internal legal and governance controls. This includes putting a DPIA in place, providing guidance to their users and publishing appropriate privacy information to patients.

The following should also be considered for local adoption and shared with users where applicable in conjunction with local information governance guidance.

Teams / Chats

- Microsoft Teams can be used for private 1:1 chats and group chats without the need to create a team.
- Any instant messages (IMs) received by a user whilst offline will be available next time that user goes online.
- Conversation history and chats are persistent, meaning conversations remain even after closing the application.
- Users must not share sensitive information within a chat unless it is intended for all **invited participants**. Invited participants will be able to read the chat even if they do not join the meeting, or if they have already been disconnected.
- Use a separate email or Teams chat for private conversations amongst a sub-group of colleagues.

Files use

- When a Microsoft team is created, a SharePoint site is also automatically created. Each channel within that team will correspond to a folder within the SharePoint site.
- Any files that are shared within a Teams chat or via the channel's files tab is automatically added.
- Any permissions are translated from the SharePoint site directly to the Teams site.
- In order to create a new document as a tab, it must first be uploaded otherwise the file will not be available to add.

Teams privacy settings

- Teams are initially created by an LA who then sets up owners of each team. Owners do not need to be an LA and they are able to manage the team, for example by adding / removing members.
- By default, all teams are created as 'private', meaning only those invited to it are the only people who have access to the shared information.

- Initially within Teams it was possible for an LA to make a team site ‘public’, meaning any NHSmail user regardless of organisation would have full access to any documents uploaded to the team site (or its underlying SharePoint site) enabling them to view, search, edit and delete information.

  To avoid accidental toggling of this setting, the functionality has been removed from LAs. Any organisation wishing to make a team site 'public’ should contact feedback@nhs.net

- Any LA with a team’s site set to ‘public’ is strongly recommended to review the requirement for this setting and any content that is locally added to the site.

- Should an LA with a public team site wish to make it private, they can do so within the NHSmail portal.

Teams data protection

- Additional information on Teams data protection in transit and at rest is available on Microsoft’s website:

  https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide

  https://docs.microsoft.com/en-us/microsoftteams/shared-device-security-for-microsoft-teams

- Teams guidance is available on the NHSmail support site.

Step 3: Consultation process

The NHSmail service has been designed in context with the Data Protection Act with reviews held in recent years to ensure processing and guidance is uplifted to reflect the new GDPR legislation – Data Protection Act (DPA) 25 May 2018.

Consulted stakeholder groups

- NHSmail Board
- Local Administrators
- All NHSmail users

The NHSmail service DPIA was produced in conjunction with the above consulted stakeholder groups and NHS Digital assurance specialists within the Strategy, Policy and Governance team of the Office of the Senior Information Risk Owner (SIRO) and is available on the NHSmail support site.

Step 4: Assess necessity and proportionality

There is a clear legal basis for the processing of personal identifiable data and / or sensitive data through the NHSmail service in the context of GDPR.

Department of Health and Social Care mandate

The NHSmail service is provided by NHS Digital (as joint controller with local organisations) via a five-year contract with Accenture (processor) with an end date of 31 March 2021.

The terms and conditions set out in the contract, which have been uplifted in accordance with GDPR legislation via Variation Notice 12, stipulate that data must be processed in accordance with the:

- Data Protection Act (1998)
- UK Data Protection Bill (14 Sep 2017)
- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
- Working Party 29 guidelines determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, wp248rev.01
- Data Protection Act (2018)

Department of Health and Social Care direction

NHS Digital has a legal obligation (a direction issued by the Secretary of State for Health and Social Care) that requires it to establish and operate informatics systems, and to exercise systems delivery functions including NHSmail as the national secure email service approved for sharing sensitive information.

The legal basis for processing, collecting, sharing and analysing data is the direction issued by the Secretary of State for Health and Social Care where NHS Digital is appointed as the service provider for NHSmail, taking responsibility for setting up and managing the data processing contract for the service on behalf of all controllers.

The NHSmail service requires individuals to agree to their personal data being managed by the NHSmail service by accepting the Acceptable Use Policy (AUP) when their account is first initiated.

Local organisations using NHSmail are required to ensure their staff have read and understood the AUP provided by the NHSmail service.

The Transparency / Fair Processing Information sets out how the NHSmail service complies with GDPR and should be used by NHSmail users in conjunction with the Transparency / Fair Processing Information provided by their local organisations (as joint controllers).

Data quality and accuracy for content sent over Teams or stored within other collaboration tools is the responsibility of the user sending / uploading the information. In the event it is incorrect the user should update and re-send / upload the corrected information.

Users should also operate within the IG guidance and policies of the employing NHS organisation.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals (include associated compliance and corporate risks as necessary).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Local NHS organisation not having their own local IG policy / procedure in place to support the processing of requests.	**Remote**	**Minimal**	**Low**
When an employee employed by organisation 'A' moves to organisation 'B', the employee is permitted, due to their O365 collaboration tool contents not being purged, to take with them the personal data for which organisation 'A' remains the controller.	**Remote**	**Minimal**	**Low**
When using Teams, SharePoint and OneDrive a user could download sensitive information to personal mobile devices.	**Remote**	**Minimal**	**Low**

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in Step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Local NHS organisation not having their own local IG policy / procedure in place to support the processing of requests.	Refer local NHS organisations and Local Administrators to NHSmail information management policies https://support.nhs.net/article-categories/information-management-policies/	**Reduced**	**Low**	**Yes**
Impact to individual data from user belonging to a new organisation and having access to an O365 account where previous	Reiterate local NHS organisation responsibility to ensure local IG policy and procedure in place to support requests. NHSmail publishes policy and guidance for how local NHS organisations can support via the joiners and leavers guide (https://support.nhs.net/knowledge-	**Reduced**	**Low**	**Yes**

organisation remained the data controller.	base/leavers-and-joiners-guide/) which sets out specific tasks that LAs must do in the event someone leaves their organisation. The NHSmail Acceptable Use Policy must be accepted by a user prior to a user sending any data. The policy states to follow IG policies of the local organisation and ensure personal email is clearly identified.			
When using Teams, SharePoint, and OneDrive a user could download personal identifiable data and / or sensitive data to personal devices.	When possible, it is recommended Organisations make use of a Zero Trust approach to client devices making use of device management capabilities, device health checks and policy enforcement, device-level encryption, and other security features. Use device encryption and ensure every user has a unique login onto a device so other users do not have access to any cached data that may persist after they close an application. If Teams is to be used on a device not under local IT management, users should only use the web browser in Incognito mode in Google Chrome or InPrivate browsing in Microsoft Edge, logging out/closing the browser at the end of their session. This will ensure no data is locally cached at the end of the session. Users on an unmanaged device should also not use the OneDrive client to download any content locally. Users should be encouraged to save content to the SharePoint site and view/edit from within a browser to ensure content is always protected in transit and at rest.	**Reduced**	**Low**	**Yes**