NHS 365

A Strategic White Paper on Maximising the Value of the Microsoft 365 National Agreement

Enterprise 365 Adoption Blueprint for Healthcare

Best Practices for Microsoft 365 Adoption Across Large Healthcare Organizations

Executive Summary

The National Health Service (NHS) stands at a pivotal moment in its digital transformation journey. With an estate of over 1.3 million staff, thousands of organisations, and one of the largest and most complex technology landscapes in the public sector, the successful adoption of modern cloud productivity and collaboration tools has never been more critical.

This report, NHS 365 – Best Practices for Adoption of Microsoft 365 Across the NHS, distils lessons learned from early-adopter trusts, the NHS 365 national team, Microsoft public-sector engagements, and comparable health systems worldwide.

It provides practical, evidence-based guidance for clinical commissioning groups, trusts, ICS digital teams, and national programme leads on how to move beyond deployment to genuine enterprise-wide adoption and cultural change.

NHS 365: A Strategic White Paper on Maximising the Value of the Microsoft 365 National Agreement

The National Health Service (NHS) stands at a pivotal moment in its digital transformation journey. With an estate of over 1.3 million staff, thousands of organisations, and one of the largest and most complex technology landscapes in the public sector, the successful adoption of modern cloud productivity and collaboration tools has never been more critical.

Microsoft 365 (M365) has been selected as the strategic platform to replace aging on-premise systems, deliver a unified digital workplace, and enable new ways of working that put patients, clinicians, and administrative staff at the centre of care delivery.

NHS 365 represents the collective national programme and local initiatives designed to accelerate the safe, effective, and equitable adoption of Microsoft 365 tools – including Exchange Online, SharePoint, OneDrive, Microsoft Teams, and the broader Power Platform and security capabilities – across NHS trusts, integrated care systems (ICSs), primary care, and national bodies.

The analysis demonstrates that the platform, when optimally deployed, is a critical enabler for achieving the NHS's core strategic goals, but that its value is contingent on solving specific challenges related to governance, interoperability, and workforce change management.

The analysis presented in this white paper is based on a comprehensive review of primary and secondary sources, including:

- Official NHS Digital Strategies: Documents outlining the national vision, including 'A plan for digital health and social care' and the "Digitise, Connect, Transform" strategy.
- N365 Agreement Technical Documentation: Specifications detailing the components, scope, and security features included in the national Microsoft agreement for the NHS.
- National IT Infrastructure and Workforce Reports: Parliamentary, NHS Providers, and British Medical Association (BMA) reports identifying persistent challenges in funding, infrastructure, interoperability, and digital literacy.
- NHS Information Governance (IG) Policies: A detailed review of the non-negotiable compliance landscape, including the Caldicott Principles, the Data Security and Protection Toolkit (DSPT), and national guidance on data residency and cloud use.
- Implementation Case Studies: In-depth analysis of M365 and Azure implementations at pioneering NHS Trusts, providing proven blueprints for success and "lessons learned" in clinical and administrative domains.

Intended Audience: This report is prepared for senior NHS leadership and strategic decision-makers, including:

- Chief Information Officers (CIOs)
- Chief Clinical Information Officers (CCIOs)
- Chief Operating Officers (COOs)
- Directors of Transformation and Digital Strategy
- Information Governance (IG) Leads and Caldicott Guardians
- Integrated Care Board (ICB) and NHS England Executives

Executive Summary: The 1.5 Million User Opportunity

The National Health Service has made a monumental investment in its digital future. The N365 agreement provides Microsoft 365 licenses to over 1.4 million users, a figure now cited as 1.5 million doctors, nurses, clinicians, and support staff. This agreement furnishes the entire health service with a unified, secure, and modern platform, representing one of the most significant technology procurements in NHS history.

However, this report finds that the value of this platform is critically underutilised. Adoption remains fragmented, and usage is often confined to basic email and chat functions. The core NHS digital strategy is to "Digitise, Connect, Transform".

The N365 agreement has rapidly accelerated the 'Digitise' phase, but the service as a whole is failing at 'Connect' and 'Transform'. This failure stems from a persistent lack of interoperability with fragmented legacy systems and, most importantly, a widespread failure to re-engineer clinical and administrative processes around the new tools.

This report argues that the primary barriers to "best use" are not technological but human and structural. True transformation is being blocked by:

1. Inadequate Change Management: A lack of structured, funded programmes to manage the "people side" of the technology shift.
2. Low Digital Literacy: Persistent skills gaps across the workforce that prevent staff from moving beyond basic tasks.
3. The EPR Chasm: A critical failure in many Trusts to build the necessary technical bridges between the M365 platform and core Electronic Patient Record (EPR) systems.

The potential, however, is transformative. A recent NHS pilot of M365 Copilot (Generative AI) alone suggests potential savings of "400,000 hours of staff time per month". Furthermore, pioneering Trusts, such as Barnsley Hospital NHS Foundation Trust and Cambridgeshire and Peterborough NHS Foundation Trust, have already created proven, replicable blueprints for success in virtual care integration and legacy data management, respectively.

This white paper provides the strategic framework to bridge the gap between potential and reality. It details actionable strategies organised into four key parts:

1. Transforming Clinical Delivery: Leveraging M365 for integrated virtual care, secure

Multi-Disciplinary Team (MDT) collaboration, and solving the EPR interoperability challenge.

2. Re-engineering Administrative Operations: Using the Power Platform and Generative AI to automate manual processes, reclaim staff time, and establish a "single source of truth" for content.
3. Establishing Watertight Governance: Building a robust compliance framework using Microsoft Purview to enforce the Caldicott Principles, the DSPT, and data residency requirements.
4. Executing a People-Centric Implementation: Creating a national-to-local implementation model based on formal Adoption and Change Management (ACM), a "Digital Champions" network, and a governing Centre of Excellence (CoE).

The N365 agreement was initially celebrated for its "significant cost savings" on licenses. This report demonstrates that this view is myopic. The procurement success is irrelevant; the most pressing NHS challenges are operational pressures, staff burnout, and profound productivity deficits. The true business case for N365 is not in license savings but in its potential to unlock millions of hours of clinical and administrative time. This reframes the entire N365 project from an IT upgrade to a strategic workforce capacity imperative.

The N365 Platform: A New Central Nervous System for the NHS

From Software to Strategic Asset

The N365 agreement must not be mischaracterised as a simple software update. It is a comprehensive, integrated platform that provides the foundational technology to execute on the NHS's core strategic documents, including the 10-Year Health Plan's shift "from analogue to digital" and the ambitions set out in 'A plan for digital health and social care'. It is, in effect, the new standard digital environment for the NHS.

Deconstructing the N365 Agreement

The national deal, negotiated by NHSX and NHS Digital, provides a baseline suite for over 1.4 million users across more than 450 organisations, including Trusts, Clinical Commissioning Groups (now Integrated Care Boards), and Health Informatics Services. While licensing tiers vary, the core components available to the NHS are:

- Productivity Suite (Office 365): This includes the standard applications (Word, Excel, PowerPoint) and, most critically, the core collaboration tools of Outlook for email and Microsoft Teams for communication.
- Modern Operating System (Windows 10/11): This moves the NHS desktop estate onto a secure, "evergreen" operating system, removing end-of-life software and standardising the user environment.
- Advanced Security: The agreement includes Advanced Threat Protection (ATP) capabilities, which provide a critical defence against sophisticated cybersecurity threats like phishing and ransomware.
- Identity and Access Management: A unified "NHS-wide directory" (now Microsoft Entra ID) provides the foundation for identity management, access control, and a single, secure login for staff.
- On-Premise Bridge (Server CALs): The deal includes Windows Server Client Access Licensing (CALs) to replace the dangerously outdated 2008R2 Server CALs.

The inclusion of Windows Server CALs is a frequently overlooked but critically important component. It is a pragmatic and deliberate acknowledgement that the NHS cannot simply become "cloud-only."

Critical "local and national clinical and administrative systems" will continue to run on-premise on Windows Servers for the foreseeable future, often due to the limitations of legacy clinical applications. The N365 agreement is not a "cloud-first" dictate; it is a hybrid-management solution.

The true central nervous system of the platform is the identity and access management layer,

which acts as the digital bridge. It allows a user with a single, secure NHS identity to access both modern cloud applications (like Teams) and, via the new CALs, the legacy on-premise clinical systems they still depend on.

The strategic goal of this platform is to provide the "strong digital foundations" that the NHS has lacked for decades. It creates the stable, secure, and standardised environment necessary to finally move away from the fragmented, paper-based systems and pursue the national "digitise, connect, transform" model.

Table 1: The N365 Component Value Matrix (NHS Context)

This table provides a summary for leaders to understand the strategic purpose of each N365 component within a specific NHS context.

M365 Component	Core Function	Primary Clinical Use Case	Primary Administrative Use Case	Key IG Consideration
Microsoft Teams	Secure communication & collaboration hub	Virtual MDTs: Securely manage cases with Planner, SharePoint, and EPR tabs. Virtual Consultations: Secure video visits with patients using MS Bookings.	Project Management: Track transformation projects. Live Events: All-staff briefings for up to 10,000 attendees.	External guest access for multi-agency collaboration must be governed by strict policies.
Power Platform (Apps & Automate)	Low-code app development & process automation	Clinical Apps: Bed management systems, biopsy tracking. Data Capture: Rapidly build forms for clinical data entry.	Process Automation: HR onboarding, invoice automation, financial reporting.	CSO Mandate: Any patient-facing app must have a Clinical Safety Officer (CSO) risk assessment.
SharePoint	Document/cont	Clinical Policy	Policy Lifecycle	Version control

Online	ent management & intranet	Hub: Single source of truth for all guidelines and policies.	Mgt: CQC-defensible workflows for document approval. Staff Intranet: Central hub for news and resources.	and audit trails are critical for clinical safety and CQC compliance.
Microsoft Purview	Data governance, risk & compliance	Data Classification: Applying 'Patient Confidential' sensitivity labels to all patient data.	Audit & eDiscovery: Finding data for IG/legal requests. DLP: Preventing accidental data leaks.	Legal Mandate: Required to enforce Caldicott Principles and meet DSPT standards.

Part I: Transforming Clinical Service Delivery

The New Consultation Room: Virtual Care and Telehealth

The COVID-19 pandemic forced a rapid, chaotic adoption of telehealth. While this accelerated digital use, it left a problematic legacy.

Many Trusts are now running "clunky," inefficient video solutions that require "a lot of manual rekeying". Furthermore, contracts for third-party tools like "Attend Anywhere" are expiring, leaving Trusts with a strategic choice: procure a new, costly point solution or rationalise onto their existing N365 platform.

The N365 license provides a superior, integrated, and cost-effective (as in, already-paid-for) solution. The "Virtual Visits" application combines Microsoft Bookings with Microsoft Teams. This provides a secure, end-to-end platform for scheduling, managing, and conducting remote consultations. Its features include:

- **Secure Scheduling:** MS Bookings provides a scheduling tool that integrates with clinicians' existing Outlook/Teams calendars.
- **Patient-Friendly Access:** Patients receive a custom link and can join from any device without needing to sign in.
- **Integrated Platform:** Clinicians manage their entire day—virtual visits, MDTs, and admin work—from the single Teams application.

Best Practice Deep Dive - Barnsley Hospital NHS Foundation Trust:

The Barnsley Hospital case study provides the national blueprint for a successful virtual care implementation.

The Trust faced the common problem of a "clunky" and "not very patient-friendly" legacy system that clinicians found frustrating. Their solution was not just to "turn on Teams," but to build an integrated platform using Power Platform and Teams, hosted on Microsoft Azure.

The success of this project hinged on three critical factors:

1. **Seamless EPR Integration:** This was the most important element for clinician adoption. An appointment created in the Trust's Electronic Patient Record (EPR) system automatically and immediately appears in the clinician's Microsoft Teams calendar. The clinician clicks to join the call from within their familiar EPR environment, completely eliminating the "manual rekeying" that caused "a great deal of frustration".
2. **Radical Patient Simplicity:** The Trust initially offered patients a choice between the

Teams app and a web browser. This proved to be a mistake, "adding unnecessary complexity" and causing patients to "get stuck". Based on this feedback, they simplified the patient journey to a browser-only link, giving the patient "zero cost of entry".

3. **Clinician-Led Design:** The project was piloted with the Speech and Language Therapy (SLT) team. Their direct feedback led to crucial enhancements, such as a "one-click" telephone backup (using Azure Communication Services) for patients who were struggling to connect to the video call.

The adoption of Microsoft Teams for virtual consultations has been "slower than initially expected" across the NHS.

The Barnsley case study definitively explains why. Success is not a technology problem; it is a workflow and user experience problem. Trusts that simply "turn on Teams" and instruct staff to use it will fail due to clinician friction (EPR rekeying) and patient friction (complex joining instructions).

The "best use" of N365 for telehealth requires a non-negotiable commitment to deep EPR integration and a human-centred design approach that obsesses over simplifying the patient journey.

The Virtual Ward and MDT Hub: Secure Clinical Collaboration

Multi-Disciplinary Team (MDT) meetings are the cornerstone of modern care for complex cases, such as in cancer or community neurology.

However, they are logistically crippling. As one community neurology team reported, the "logistics around time and space to meet face to face" are "often too time consuming and not often practicable". The traditional "before" state of MDT collaboration consists of fragmented, non-auditable chains of separate emails and telephone calls.

Microsoft Teams provides the "virtual hub" to solve this. The NHS has a purpose-built "Virtual MDTs App" available on the N365 shared tenant. When a new MDT is required, this app template can instantly create a secure, pre-configured Team with:

- Channels: Organised sub-topics for structured collaboration.
- SharePoint Folders: A secure, access-controlled location for sharing patient-specific documents and files.
- Microsoft Planner: A board to manage, assign, and track the tasks and actions for a patient's care plan.
- EPR Tab: A dedicated tab that can display the web-based version of the Electronic Patient Record.
- Virtual Whiteboard: A collaborative space for clinicians to annotate and brainstorm during meetings.

This solution fundamentally transforms the nature of an MDT. It moves the MDT from being a single, inefficient, synchronous meeting to a persistent, asynchronous care hub. Before the N365 solution, clinicians had to waste valuable meeting time gathering and presenting data. With the N365 solution, a specialist can review a patient's files (in SharePoint) and add notes to the care plan (in Planner) before the scheduled meeting.

The "meeting" itself then becomes a rapid, high-value decision-making forum, focused only on complex cases. This directly answers the national call to "streamline" MDTMs and ensure "optimum use of clinical time".

Bridging the Chasm: A Strategy for EPR and Legacy System Interoperability

The Core NHS Challenge: The single greatest barrier to digital transformation in the NHS is the "lack of interoperability". The National Audit Office (NAO) and parliamentary reports have repeatedly identified this as the primary reason for "expensive and largely unsuccessful" digital projects over the past 20 years. The NHS is a landscape of data silos, where different systems "cannot 'speak to' each other". N365, if implemented in isolation, risks becoming just one more silo.

The Strategy: The N365 platform must become the connective tissue that bridges these silos. This requires a two-pronged approach:

1. Live Integration (The "Hot" Data): This involves connecting M365 tools directly to the live EPR. This is achieved using modern interoperability standards like FHIR (Fast Healthcare Interoperability Resources). Microsoft provides a "Teams EHR connector" that enables this link for major EPRs like Oracle Health (Cerner) and Epic, allowing clinicians to launch a virtual visit from the patient record, as demonstrated by the Barnsley case study.
2. Legacy Data Integration (The "Cold" Data): This involves managing the decades of patient data locked in legacy systems.

Best Practice Deep Dive - Cambridgeshire & Peterborough FT (CPFT):

The CPFT case study provides a game-changing, nationally significant blueprint for solving the "cold data" problem.

- The Problem: In 2020, CPFT was migrating to a new EPR. They had 23 years of "unwieldy" legacy data (from 1997-2020) spread across a clinical data library and an old RiO EPR system. This amounted to over three million clinical documents.
- The "Old Way" (The Problem): The standard NHS approach is a "lift and shift" migration. The new EPR vendor's plan for this was estimated to take 48 weeks. An outside supplier's quote was "too expensive," at "£250k per data feed". This costly, slow approach is the default for most Trusts.
- The "New Way" (The Solution): CPFT's internal team, with Microsoft's advice, took a radical

new approach. They moved all three million legacy documents and structured data into a Microsoft Azure cloud storage solution (the same secure cloud that underpins N365). They then applied Azure Cognitive Search (now Azure AI Search) over this entire dataset.

- The Outcome: The Trust saved approximately "£700k on the install costs" and went live in a fraction of the time. Clinicians now have a secure, single-sign-on webpage that sits alongside their new EPR. This webpage allows them to perform a keyword search across 23 years of data—including scanned handwritten notes and PDFs—and get results in "literally three seconds". Clinicians described the performance as "mind blowing" and "game changing".

This "Search and Archive" strategy, enabled by the M365/Azure platform, is profoundly superior to the traditional "Lift and Shift" migration. It is faster, dramatically cheaper, and more effective (e.g., searching handwritten text). It is a repeatable blueprint that every NHS Trust facing an EPR migration or dealing with a legacy data archive should adopt. It solves one of the oldest and most expensive problems in NHS informatics.

Part II: Re-engineering the NHS Back Office

While clinical transformation is the ultimate goal, the NHS is suffocating under a parallel crisis of administrative burden. Staff are mired in "inefficient workflows," "costly legacy software," and "repetitive, time-consuming tasks". The N365 platform provides the tools to automate this non-clinical work, freeing up resources and improving staff morale.

Automating the Administrative Burden: The Power Platform

Every NHS Trust runs on thousands of manual, paper- or spreadsheet-based processes for critical functions like HR, finance, and operational management. These processes are slow, prone to error, and consume vast amounts of staff time.

The Power Platform (included in N365) is a "rapid application development environment" designed specifically to solve this. It allows staff—even those without coding skills—to build custom apps and automate workflows.

- Power Apps: This tool allows "citizen developers" to build custom applications. NHS Trusts are already using this to build solutions for:
  - Clinical Operations: "Bed Management" systems and "Biopsy Tracking (Histopathology)".
  - Data Automation: "POCT (Point of Care Testing) Data Automation".
- Power Automate: This tool automates workflows across different applications. It includes Robotic Process Automation (RPA) for "high volume, rule-based, repeatable tasks". Existing NHS use cases include:
  - Finance: "Invoice Automation" and automated financial reporting.
  - HR: Automating "onboarding/offboarding" and "staff transfers".
  - Patient Admin: Appointment scheduling and report generation.

The very power of this platform—that "business users can easily create, modify, and track processes"—is also its single greatest risk. An ungoverned, "Wild West" adoption of the Power Platform will create a new, chaotic, and clinically unsafe generation of shadow IT.

The NHSmail support documentation provides explicit, non-negotiable governance mandates that all Trusts must follow:

1. Environment Risk: Creating an app in the "NHS default environment" is a critical error, as it "will be visible to everyone on the NHSmail shared tenant". This is a severe data breach risk.
2. Environment Control: Trusts must use separate "Sandbox" (for development/testing) and "Production" (for live use) environments to manage the application lifecycle.

3. Clinical Safety Mandate: This is the most crucial rule: "Where an organisation uses Microsoft Power Apps to develop an application for use within a patient care pathway," it must appoint a Clinical Safety Officer (CSO) and conduct a "comprehensive clinical risk assessment".

This means the "best use" of the Power Platform is not uncontrolled innovation. It is governed innovation, managed by a formal Centre of Excellence (see Section 6.4) and subject to rigorous clinical safety oversight.

From Paper-Based to 'Single Source of Truth': SharePoint Online

The "paperless NHS" objective is unachievable as long as Trusts rely on fragmented, insecure shared network drives or, worse, paper binders for critical information. This creates significant clinical risk and regulatory liability, as staff may access outdated policies or procedures.

SharePoint Online is the platform designed to solve this. It is not just a "shared drive in the cloud." It is a comprehensive system for building a "secure hub for collaboration, communication, and document management".

Its core function, in a clinical governance context, is document lifecycle management. SharePoint provides the tools to control the entire life of a critical document (e.g., an infection control policy):

- Creation: Using a standard template.
- Review & Approval: Using integrated workflows.
- Publication: Making only the single, approved version visible to all staff.
- Disposition: Archiving or deleting the document when it is superseded.

This capability is a core clinical safety and CQC compliance tool. When a regulator like the CQC inspects a Trust, a key line of inquiry is "Are your policies and procedures up-to-date, and can staff access them?"

- The "Old Way" (The Problem): "Our policies are on the 'G:' drive." This is an indefensible, chaotic answer.
- The "N365 Way" (The Solution): "All clinical policies are managed in this SharePoint Online library. We have automated workflows for review and approval. We use 'version control' to ensure staff can only see the single, correct, current version. We have a full audit trail for every document."

This transforms SharePoint from a simple file store into a defensible governance, risk, and compliance platform.

The Generative AI Co-pilot: Unlocking Administrative Productivity

The Challenge: The administrative burden in the NHS is a key driver of low productivity and staff burnout. Staff at all levels, from clinicians to back-office-teams, spend hours on low-value tasks like summarising meetings, drafting communications, and managing emails.

The N365 Solution: Microsoft 365 Copilot is a generative AI assistant integrated directly into the M365 applications that staff "use daily, such as Microsoft Teams, Outlook, Word, Excel and PowerPoint".

- The Potential: A groundbreaking NHS pilot in 2023 across 90 organisations yielded staggering results. It found that Copilot could save "on average 43 minutes per staff member per day".
- The Scale: Extrapolated across the NHS, this "could save up to 400,000 hours of staff time per month," which equates to "millions of hours every year". This is time that can be refocused "on frontline care". Use cases include instantly transcribing and summarising the salient points from a patient consultation or MDT meeting.

The immediate and correct question from every NHS leader, CIO, and Caldicott Guardian is: "Is this safe? Is my patient data being sent to OpenAI to train the model?" The adoption of this tool is 100% dependent on the answer.

The technical architecture of M365 Copilot provides critical, explicit reassurances. This "Trust Architecture" is its most important feature:

1. No Data is Used for Training: Microsoft's documentation states unequivocally: "Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs".
2. Data Stays within the Tenant Boundary: All data processing for M365 Copilot "is processed within the Microsoft 365 service boundary". This means the data does not leave the NHS's secure, UK-based tenant (see Section 5.3).
3. Permissions and Labels are Inherited: This is the key to its safety. Copilot is not an all-seeing AI. It is an extension of the user. It "respects your identity model and permissions" and "inherits your sensitivity labels".

This final point means that a user cannot use Copilot to find or summarise data they do not already have permission to access. Furthermore, if a document is labelled "Highly Confidential - Patient Data" (see Section 5.2), Copilot inherits and respects that label and its associated encryption and sharing restrictions. This "governance by design" is the fundamental prerequisite that unlocks the safe, responsible use of generative AI in the NHS.

Part III: A Framework for Trust and Security

The N365 platform is not just a productivity suite; it is a comprehensive security and governance platform. For the first time, the NHS has a unified, modern toolset to enforce its complex information governance rules, moving them from passive policies in a binder to active, automated technical controls.

Information Governance by Design: Applying NHS Standards to M365

The Mandate: All use of the N365 platform is non-negotiably bound by UK law (Data Protection Act 2018), the Common Law Duty of Confidentiality, and all NHS information governance standards.

The Frameworks: The implementation must be built to comply with two core frameworks:

1. The 10 Data Security and Protection Toolkit (DSPT) Standards.
2. The Caldicott Principles.

To begin, all Trusts must complete a Data Protection Impact Assessment (DPIA) for their local M365 implementation, using the templates provided by NHS England.

A common misconception is that a cloud platform like M365 increases IG risk. The reality is the opposite. A properly configured M365 tenant provides superior and more defensible compliance than legacy systems. It provides the technical tools to enforce the Caldicott Principles, moving them from abstract concepts to concrete practice.

- Caldicott Principle 1 (Justify the purpose): M365's comprehensive audit logs provide a clear, auditable record of who accessed what data, when, and (via context) why.
- Caldicott Principle 3 (Use the minimum necessary): M365 technical controls like "Information Barriers" and granular, role-based access can physically prevent a user from accessing data that is not necessary for their role.
- Caldicott Principle 4 (Access on a strict need-to-know basis): This is the core of M365 security. Access to a "Team" for a 'Urology MDT' or a SharePoint site for 'HR' is explicitly controlled and restricted only to verified members of that group. This is infinitely more secure and auditable than paper files in an unlocked office or patient data on a widespread "all-staff" shared drive.

This means an Information Governance lead can, and should, be more confident in their compliance posture with a well-governed M365 tenant than with any legacy on-premise or paper-based system.

Table 2: M365 Information Governance (IG)

Compliance Map

This table serves as a practical tool for IG leads and CIOs to demonstrate to auditors, their board, and the CQC how M365 tools map to and fulfill specific NHS compliance mandates.

NHS Mandate	Requirement	M365 Technical Control	How it Fulfills the Mandate
Caldicott Principle 4	Access on a strict need-to-know basis.	Microsoft Entra ID Conditional Access & Group Policies	Access to a "Team" (e.g., 'Cardiology MDT') or SharePoint site is restricted only to the verified, named members of that clinical group.
DSPT Standard 4	Managing data access.	Microsoft Purview Sensitivity Labels	Data identified and labelled as 'Patient Confidential' can be automatically encrypted, access can be logged, and sharing can be restricted.
DSPT Standard 9	IT protection.	Microsoft Advanced Threat Protection (ATP)	Actively scans emails and links for sophisticated phishing and ransomware attempts, protecting the tenant from external attack.
NHS Data Loss Risk	Accidental sharing of Patient Identifiable Data (PID) to an external email.	Microsoft Purview Data Loss Prevention (DLP) Policy	The policy actively scans outbound emails/files for sensitive identifiers like "UK National Health Service Number" and will block or warn the user before the breach occurs.

Common Law Duty of Confidentiality	Ensuring patient information is not disclosed without a legal basis.	Microsoft Purview Information Barriers	Can be configured to create digital "walls" between teams (e.g., preventing a research team from ever communicating with a clinical team via Teams chat) to manage conflicts of interest and ensure data segregation.

Protecting Patient Data: Microsoft Purview and DLP

The N365 platform includes Microsoft Purview, the suite of tools that operationalises the governance framework described above. Its two most critical components for the NHS are Sensitivity Labels and Data Loss Prevention (DLP).

1. Sensitivity Labels:

Trusts must define and deploy a simple, clear hierarchy of "sensitivity labels" (e.g., 'Public', 'Internal', 'Confidential', 'Highly Confidential - Patient Data'). These are not just visual stickers; they are digital tags that travel with the data wherever it goes. Applying the "Patient Data" label can be configured to automatically:

- Encrypt the document.
- Apply a watermark.
- Block sharing with external users.
- Inform Copilot that this data is highly sensitive.

2. Data Loss Prevention (DLP):

DLP policies use these labels and other data identifiers to actively prevent data breaches at the point of exit. The NHSmail guidance provides a perfect, practical example of this in action:

1. A clinician drafts an email or tries to share a file from OneDrive/SharePoint with an external recipient.
2. The DLP policy actively scans the content and "identif[ies] sensitive information" based on a pre-defined list, which includes "UK National Health Service Number," "Credit Card Number," or "UK Driver's License Number".
3. A "DLP pop-up" "prompt[s]" the user, warning them that they are about to share sensitive information.

4. The user is given the option to "Override" the block, but they must provide a business justification, which is logged.
5. This override action is sent to an IG/Security team for-post incident review.

This single workflow represents a monumental shift in data protection. It moves governance from a passive model (e.g., "I vaguely remember my annual training") to an active model (e.g., "A pop-up is warning me right now that this email is a mistake").

However, governance leads must be aware that this protection is not ubiquitous. As of 2019, M365 tools like "Sway" and "Microsoft Forms" did not support DLP or eDiscovery. This creates a critical governance gap. Trusts must implement policies that restrict the use of these specific, non-compliant applications for the collection or sharing of any Patient Identifiable Data (PID).

Data Sovereignty: Managing Data Residency and Security

NHS national guidance on the use of public cloud services is explicit and strict: "Data must only be hosted within the UK". Any use of a cloud service that stores data "outside of the UK," (e.g., in the European Economic Area (EEA) or the United States), requires explicit approval from a Senior Information Risk Owner (SIRO) and a comprehensive risk assessment.

Microsoft 365 is a global "hyperscale" cloud service. While Microsoft maintains UK data centres and core data for services like SharePoint and Exchange are often stored there by default, this is not a contractual guarantee for all data in all services.

The Microsoft 365 Advanced Data Residency (ADR) add-on. This add-on is not a new piece of software; it is a contractual commitment. For customers in an eligible country (which includes the United Kingdom), the ADR provides a binding service-level agreement that "Customer Data" for a specific list of services will be stored only in that local region.

Critically, the list of services covered by the ADR add-on includes:

- Exchange Online
- SharePoint and OneDrive
- Microsoft Teams
- Microsoft 365 Copilot
- Microsoft Purview (Audit, DLP, Information Protection)

This is a point of paramount strategic importance. For the NHS to safely and compliantly adopt the entire N365 suite—especially the AI-powered Copilot—it must have this contractual guarantee of UK data residency. Without the ADR add-on, individual Trusts could be non-compliant with the national data hosting policy.

Therefore, NHS England must provide central confirmation that the national N365 agreement includes the Advanced Data Residency add-on for all Trusts. This central assurance is the key that unlocks platform-wide, data-secure adoption.

Part IV: The Implementation Blueprint: A People-First Strategy

The N365 licenses have been procured. The technology is available. Yet, adoption remains slow and fragmented. This is because the final, and most difficult, challenge is not technical. The "primary barrier to digital adoption" in the NHS is "workforce-related issues, rather than technology". Operational pressures, a lack of "clinical engagement", and low digital confidence are the true blockers.

This section provides a four-part blueprint for a people-first implementation strategy.

Overcoming the Human Barrier: Adoption and Change Management

The Core Problem: The NHS has a history of failed IT projects that were rolled out with a "big bang" approach—a technical deployment, a single all-staff email, and an optional training video. This "deploy and pray" model is what leads to "stagnated" adoption and "utter frustration".

The Successful Model: Adoption & Change Management (ACM): The N365 rollout must be funded, resourced, and executed as a people and culture change programme, not an IT project.

Best Practice Deep Dive - Insight NHS Trust Implementation:

A case study of an NHS Foundation Trust with 6,500 employees provides a clear model for success.

- The Problem: The Trust's on-premise infrastructure was ending support. Staff were spread across multiple sites, working in "silos," and a growing "shadow IT" problem (using unapproved apps) was creating a "particular threat to data security".
- The Solution: The Trust procured N365 licenses and a formal Adoption and Change Management (ACM) service. The ACM team "worked directly with the Trust's employees to understand their current ways of working and determine any frustrations, challenges, and pain points".
- The Process: Based on this, they defined a "new way of working". They did not try to train 6,500 people at once. Instead, they first trained a small "pilot group of digital champions," empowering them to "bring other users on board".
- The Outcome: This people-centric approach was a "success". "All employees... are now using the approved platform – reducing the use of shadow IT and improving productivity".

The lesson is unequivocal. NHS Trusts must re-allocate their "digital" budgets. The license cost is a small, fixed component. The majority of investment—in time, resources, and specialist

help—must be directed at the human side of the change.

Combating Shadow IT: The Digital Champions Programme

"Shadow IT" is the use of unapproved hardware or software without the knowledge of the IT department. In the NHS, this commonly includes clinicians using personal apps like WhatsApp for clinical discussions or Dropbox for file-sharing.

Staff do this for "noble reasons"—often because the "approved technology is inferior or creates more problems than it solves". This practice, however, creates a massive, unmanaged risk of data breach and regulatory failure.

The Wrong Solution: Attempting to block or ban shadow IT. This is an "outdated, ineffective approach" that drives the practice further underground.

The Right Solution:

1. Provide a superior, approved alternative (i.e., Microsoft Teams is a better, more secure platform for group chat and file sharing than WhatsApp).
2. Provide a trusted, scalable human support network to drive its adoption. This is the Digital Champions Programme.

The Model:

1. Recruit: Identify enthusiastic "super users" and early adopters from within clinical and administrative teams (not from the IT department).
2. Empower: Provide this "pilot group" with advanced training and "Art of the Possible" workshops to show them what N365 can really do.
3. Unleash: These Champions become the "approachable source of knowledge" for their peers. They "advocate new processes within their teams" and provide "at the elbow" support.

This peer-to-peer model is the only cost-effective and scalable way to support a 1.5 million-user workforce; the central IT helpdesk cannot do it. Because the Champions have "pre-existing, trusted relationships", they are far more effective at "spread[ing] the message" and understanding the "potential fears and risks" of their colleagues than a top-down corporate email from the IT department. The Insight case study provides definitive proof: the ACM team trained the champions, who then trained the wider team, successfully "reducing the use of shadow IT."

A Maturity Model for M365 Adoption in the NHS

"Digital maturity" across the NHS is low and highly variable. One 2024 report states that only 20% of NHS organisations are "digitally mature". Trusts need a clear roadmap to benchmark their current state and plan their journey.

This 5-level maturity model provides that roadmap. It shifts the focus from "what technology have we deployed?" to "how are our people working?"

Key Table 3: M365 Adoption Maturity Model for NHS Trusts

This table serves as a benchmarking tool for Trust leadership to self-assess their current state and identify the concrete steps, technologies, and governance required for progression.

Maturity Level	Name	Description (What it looks like)	Key Technologies	Governance Focus
Level 1	Basic Productivity	Staff use Outlook for email, Word for docs. Teams is used as basic instant messaging. SharePoint is an unorganised file dump (a "G: Drive in the cloud").	O365 basics	Basic password policies. IT is reactive.
Level 2	Basic Collaboration	Teams meetings are standard practice. Staff use Teams Channels for projects. Some "shadow IT" has been reduced (e.g., WhatsApp use is down).	Teams (Meetings & Channels), SharePoint (basic), OneDrive	IT-led governance. A basic Digital Champions network is formed.
Level 3	Process Re-engineering	"New ways of working" are defined. Power Apps are automating	Power Platform (Apps & Automate), SharePoint (advanced	Formal CoE is established. CSO oversight is mandatory for all

		manual admin tasks. SharePoint is a CQC-compliant policy hub.	document mgt.)	patient-facing apps.
Level 4	Integrated Clinical Platform	M365 is the "front door" for clinicians. Seamless EPR integration is live. Teams is the default platform for virtual care. Virtual MDTs are standard.	Teams + EPR Connectors, Microsoft Purview	Governance-by-Design. DLP policies are active. Sensitivity labels are deployed. Copilot is being piloted.
Level 5	Transformative & Predictive	Data from the M365/Azure platform is now a strategic asset. Azure AI is used on legacy data for clinical insights. Power BI dashboards are predictive.	Azure AI Search, Power BI (Advanced), Copilot (Full Deployment)	Data-driven, automated governance. An AI & Ethics Board is established.

Governing the Platform: The Centre of Excellence (CoE) Model

The Challenge: How does a Trust "balance innovation and control"? How can it empower clinicians to build helpful Power Apps without creating a clinically unsafe, ungoverned "Wild West" of unsupported applications?

The Solution: A Centre of Excellence (CoE). A CoE is a central team that "drives innovation and improvement... while providing standards, consistency, and governance to the organization".

The Model (Hub and Spoke):

- The Hub (National): NHS England provides the "hub." Its existing "Cloud centre of

excellence" and "Workforce Experience Centre of Excellence" are responsible for setting national standards. They provide the "Azure Well-Architected Framework" guidance, national DPIA templates, and centrally approved applications.

- The Spokes (Local): Every Trust or ICB must establish its own "spoke" CoE. This local CoE is the operational engine of governance. Its responsibilities are:
    1. Platform Management: Managing the Power Platform "Sandbox" to "Production" pipeline.
    2. Clinical Safety: Running the mandatory CSO risk assessments for all new patient-facing apps.
    3. Workforce Enablement: Training and managing the Trust's "Digital Champions" network.
    4. Monitoring: Using governance tools, like the "Power Platform CoE Starter Kit", to gain insights into app usage and manage risk.

The CoE is the practical, operational "how" for the entire governance framework. It is the engine that allows a Trust to safely progress up the M365 Maturity Model (Table 3).

Strategic Recommendations and Conclusion

This report has demonstrated that the N365 agreement provides the NHS with the tools to build a modern, efficient, and integrated health service. Success, however, is not guaranteed by the license; it must be earned through a deliberate, people-centric, and clinically-led strategy.

Failure to do so will result in a fragmented, low-adoption landscape, a monumental waste of public investment, and the persistence of the very "shadow IT" and clinical friction the platform was meant to solve. A successful strategy, as outlined in this report, will be measured in millions of hours given back to clinicians and a data-secure ecosystem that is, for the first time, truly connected.

Based on the analysis, this report provides four strategic recommendations for NHS leadership:

Recommendation 1 (For Trust CIOs and COOs): Prioritise People, Not Technology.

The M365 implementation must be re-classified as an Adoption and Change Management (ACM) programme, not an IT rollout. Budgets must be re-allocated to reflect this reality. The majority of investment should be focused on the "human factor," including the establishment of a formal, funded "Digital Champions" network. This is the primary, scalable, and most effective method to drive new ways of working, embed skills, and actively "reduce the use of shadow IT".

Recommendation 2 (For Trust CCIOs and CSOs): Govern the Power Platform, Don't Ban It.

The Power Platform is one of the highest-value tools for automating inefficient processes. It is also one of the highest-risk. Trusts must immediately establish a local Centre of Excellence (CoE) to govern its use. It must be mandated that any patient-facing Power App must undergo a full clinical risk assessment by an appointed Clinical Safety Officer (CSO) before it is moved to a "Production" environment.

Recommendation 3 (For Trust CIOs and Digital Leads): Make EPR Integration Your #1 Technical Priority.

The transformative value of M365 in clinical settings is unlocked by its integration with the EPR. Do not wait.

- For Live Data: Use the Barnsley Hospital blueprint. Prioritise the integration of Teams and the EPR (using FHIR and the EHR Connector) to create a seamless, "no-rekeying" virtual care workflow.
- For Legacy Data: Use the Cambridgeshire & Peterborough FT blueprint. Do not attempt a costly, high-risk "lift-and-shift" migration of legacy records. Instead, use Azure Cognitive Search to create a cheap, fast, and secure "searchable archive" of all legacy patient records, including handwritten notes.

Recommendation 4 (For NHS England): Centrally Mandate and Fund the "How".

The national "Digitise, Connect, Transform" strategy is sound, but individual Trusts are failing at "Connect" and "Transform." To ensure consistency and safety, NHS England must:

- Fund the "Hub": Expand the central "Cloud centre of excellence" and "Workforce Experience CoE" to provide all Trusts with baseline, pre-configured, "DSPT-compliant" templates for Microsoft Purview (Sensitivity Labels) and DLP policies.
- Guarantee Data Sovereignty: Provide central, unambiguous confirmation that the national N365 agreement includes the Advanced Data Residency (ADR) add-on. This is a non-negotiable prerequisite to ensure all Trust data—and especially all Copilot AI interactions—are contractually and compliantly "hosted within the UK".

Concluding Statement: The N365 agreement is not an "IT upgrade." It is a once-in-a-generation opportunity to build a new, unified, and secure operating system for the National Health Service. Its failure will be one of fragmented adoption, wasted investment, and persistent clinical friction. Its success, as outlined in this report, will be measured in the millions of hours given back to clinicians, in seamless administrative workflows, and in a data-secure ecosystem that finally delivers on the promise to "connect" and "transform" patient care.