Business Services Organisation

INVESTORS IN PEOPLE®
We invest in people Silver

BSO Policy on the use of Artificial Intelligence

May 2025

Policy/Procedure Development Overview

Title:	BSO Policy on the use of Artificial Intelligence		
Ownership:	Ben Doran - Director of Digital		
Equality Screened:	TBA	**BSO Policy Subgroup Consulted:**	30th October 2024 12th May 2025
Approved by:	ELT	**Date Approved:**	30th January 2025 12th May 2025
Date Implemented:	-	**Date for Review:**	Annually
Version No.	2.1	**Supersedes:**	2.0
Director Responsible:	Ben Doran - Director of Digital		
Lead Author:	Stephen Beattie	**Lead Author Position:**	Assistant Director ITS [interim]
Department:	Digital	**Contact Details:**	stephen.beattie@hscni.net
Key Words:			
Links to other Policies, Procedures & Guidance	Generative AI framework for UK Government (publishing.service.gov.uk) ai-playbook-for-the-uk-government NHS England » Artificial intelligence (AI) and machine learning Digital Technology Assessment Criteria (DTAC) - Key tools and information - NHS Transformation Directorate (england.nhs.uk) Understanding RPA - Guidance for designing, delivering, and sustaining RPA within the NHS - NHS Transformation Directorate (england.nhs.uk) RPA Guidance - Final.pptx (england.nhs.uk) Guidance on AI and data protection | ICO AI and data protection risk toolkit | ICO		

Table of Contents

Foreword

Although being a technology available for use for over a decade the public perception of artificial intelligence and its ability to change ways of working and disrupt business has grown considerably in the last year with the release of popular and easy to use commercial products. With the increased use of generative AI in the wider context, and the move across all industries to adopt automation, there is opportunity for the BSO to embrace this technology for the betterment of our staff and our customers.

It is important though to always remember that most of the data we utilise to perform our work is data we hold for our customers, some of which is sensitive in nature. It is therefore necessary that we safeguard our customers and staff and provide a set of rules around the adoption and use of AI, to ensure it is deployed safely and with a full understanding.

This policy will help staff to make informed decisions on how they can use these suites of technologies in a safe manner, and to set out specific boundaries with how we wish staff to operate. We will establish governance around the use of these technologies to support the service improvements we believe it can drive to focus on several key themes: -

- Quality
- Productivity
- Safety
- Integrity

Artificial Intelligence systems should be seen as a method of augmentation of existing people or processes, not a replacement. It is worth noting that AI will not fix an underlying process issue and should instead be considered when developing improved processes.

Links are provided within this document to existing NHS Frameworks and guidance on the usage of AI, including:-

- UK Government Generative AI Framework
- ICO AI Toolkit
- DTAC

Scope

This policy applies to use of any form of artificial intelligence and sets out the control mechanisms which must be put in place before staff use this technology for business purposes. Where a technology is not specifically listed below, the process set out to access artificial intelligence or related technologies should still be followed.

Artificial Intelligence can currently be categorised across several technologies, but given the speed of development in this area, this should not be seen as an exhaustive list.

- Generative AI
- Computational Intelligence (CI)
- Robotic Process Automation (RPA) / Hyper Automation

The current roadmap for AI regionally and a number of use case can be found in the appendix of this policy document. The strategic direction and roadmap for AI is set by Chief Digital and Information Officer (CDIO) through the NI HSC AI Steering Group.

This policy does not cover client organisations or remove their requirement for governance around the use of AI. In order to utilise AI, the client organisation(s) must manage the risk of their data through existing governance measures and sign off the risk of any AI product before the service accesses HSCNI data.

When a request is made by a client organisation (including BSO itself), the relevant controls within that organisation must be followed in addition to those controls set out within this document, in essence this document shows the minimum level of control required before undertaking a project related to AI. Additional controls and requirements within existing governance, such as the use of a DPIA, the use of a risk assessment, the use of formal change controls or business cases must also apply.

Detailed Overview

The following section provides a brief overview of the various technologies and the controls we require before said technology is put in place.

Generative AI

Generative AI can be described as an emulation of human intelligence to build products or capabilities that traditionally could only be completed by a person. The technology allows the user to quickly develop products based on learned data sets, or preexisting data sets. This is done through a combination of Algorithms, Machine Learning and Neural Networks.

The advantages of this technology are in the quality of the products and the speed of production. Generative AI can also be used to review and improve existing sources of information; for example, providing executive summaries from multiple data sources.

A detailed explanation of Generative AI can be found in the HM government Generative AI Framework.

Control

It should be noted that public Large Language Models can and do use publicly available data to generate content. Data fed to the model can also be utilised to inform future outputs. It is therefore explicitly forbidden to utilise business or customer data with public facing LLM's as this will be classified as a data breach.

It should also be noted that large LLM's are trained on unverified data and may be inaccurate or subject to bias which may negatively impact the outcome. All outputs from generative AI must be subject to human review to ensure the message is as intended. Using output from Generative AI tools without reviewing it for accuracy

places BSO at risk and may harm the organisation's reputation with the public, customers, or employees.

To maintain the BSO core value of Openness and Honesty, all content generated using Generative AI must be clearly identified on any outward-facing content (for example the use of a footnote of watermark to show that it was AI generated).

Computational Intelligence

Computational Intelligence (CI) focuses on developing AI systems capable of mimicking problem-solving abilities learned through observation and repetition. CI aims to create intelligent computer systems that learn, adapt, and excel in complex scenarios, making it a valuable component in the development of successful AI systems.

CI is typically used to review similar data sets, such as in the field of medical imaging and to provide an indicative diagnosis based on trained data sets.

Control

It should be noted that under UK General Data Protection Regulation, citizens have the right to request to not be subject to review by an automated decision-making process. Therefore, any process or tool deployed within BSO that utilises a CI, must have a compliant framework in place to allow citizens to "opt out".

Due to the nature of CI, it may require large amounts of data to be analysed loaded into the CI. The preferred deployment method for CI should be within the boundaries of the managed HSCNI platform. This platform may include cloud services owned, secured or managed by BSO.

All outputs from CI must be subject to human review to ensure the product is as intended. Using output from CI tools without reviewing it for accuracy places BSO at risk and may harm the organisation's reputation with the public, customers, or employees.

For systems that require data to be sent out from HSC to a 3rd party vendor or network, controls must be put in place to ensure the confidentiality and integrity of the HSC data is maintained. These controls should include but are not limited to:

- Must have: -
    - An agreed contractual mechanism which contains suitable controls and protections for HSC data around GDPR and cyber security.
    - A signed Data Sharing Agreement between BSO and the relevant HSCNI organisation.
    - Confidentiality agreements that data will not be used for the purpose of training the CI without express permission of the SIRO's and a supporting legislative framework by which this work can be undertaken.
    - Approval of the BSO Digital Change Advisory Board.
    - Approval of the DHCNI Enterprise Architecture Board.

    - Appropriate funding in place to cover all costs related to the CI and the hosted environment.
- Should have: -
    - External vendors should be accredited to Cyber Essential Plus, ISO 27001, or an equivalent.
    - Penetration testing of external environment within the last 12 months.

Robotic Process Automation/ Hyper Automation

Robotic Process Automation is similar in nature to CI, but instead of developing problem solving, the focus is on repetition of defined tasks through agreed processes and does not incorporate machine learning. The purpose of RPA is to complete repetitive manual task at high speed and in a consistent fashion.

RPA uses software automation (robots) to perform tasks such as data extraction, form filling, and file movement. RPA tools follow predefined workflows to complete activities and transactions.

Due to its nature, when a robot cannot complete a task in line with its predefined ruleset, the robot will await human intervention such as but not limited to: -

- Manually review and approve a record.
- Manually amend an input.
- Exclude an input from the process.

It is therefore critical that this is seen as an augmentation of a process and not a replacement of the process.

Control

Due to the nature of RPA, it may require large amounts of data to be provided to the robot for the process to execute. The preferred deployment method for CI should be within the boundaries of the managed HSCNI platform. This platform may include cloud service owned, secured, and managed by BSO. Every deployment should be subject to review through the standard governance such as but not limited to the business case process.

For systems that require data to be sent out from HSC to a 3rd party vendor or network, controls must be put in place to ensure the confidentiality and integrity of the HSC data is maintained. These controls should include but are not limited to:

- Must have: -
    - An agreed contractual mechanism which contains suitable controls and protections for HSC data around GDPR and cyber security.
    - A signed Data Sharing Agreement between BSO and the relevant HSCNI organisation.
    - Confidentiality agreements that data will not be used for the purpose of training the CI without express permission of the SIRO's and a supporting legislative framework by which this work can be undertaken.
    - Approval of the BSO Digital Change Advisory Board.

    - Approval of the DHCNI Enterprise Architecture Board.
    - Appropriate funding in place to cover all costs related to the CI and the hosted environment.
    - A completed Privacy Impact Assessment
- Should have: -
    - External vendors should be accredited to Cyber Essential Plus, ISO 27001, or an equivalent.
    - Recent Penetration testing of external environment

Acceptable Use

The following section details the guidelines by which all staff must adhere in relation to the use of Artificial Intelligence within BSO. Failure to adhere to the guidelines set out within this policy may result in staff being managed through the disciplinary process and in some cases may result in disciplinary action.

The core guidelines by which staff must act are as follows: -

- Only corporately provided tools should be utilised by staff to complete their work. These tools will be made available as and when the supporting governance has been established and will be deployed as part of an agreed corporate approach or regional project.
- Any use of AI, via platforms, tools, and software must be consistent with existing policies and applicable legislation.
- Use of AI on corporate devices must be limited to business purposes.
- Use of AI tools on personal devices or personal accounts to conduct BSO business is strictly prohibited.
- Use of AI tools on personal devices to circumvent organisation policies or safeguards is strictly prohibited.
- The request for AI tools must be managed under the existing Service Request process and is subject to review and managerial approval in relation to budget control and risk management.
- Do not use organisation credentials, email addresses, or telephone numbers as a login to publicly available AI applications on business devices or on personal devices.
- Do not install non-approved Application Programming Interfaces (APIs), plug-ins, connectors, or software related to AI systems.
- Do not input HSCNI intellectual property into non-approved AI applications.
- Do not enter personal information of patients, employees, customers, or other third parties into any non-approved applications. Treat the application as you would an employee of another organisation with whom we have no formal relationship.
- Do clearly attribute any output used for work purposes to the AI application that created it through a footnote or other means visible to the reader.

- Do maintain an updated record AI use for work purposes and be able to share those records with your manager or other authorised personnel upon request.
- Do review output of AI applications to make sure it meets Organisation's standards for principles of equity, ethics, and appropriateness.
- It is forbidden to use any output that discriminates against individuals on the basis of race, colour, religion, sex, gender, national origin, age, disability, marital status, political affiliation, without/without dependants or sexual orientation.
- It is forbidden to use AI applications to create any content e.g. text, audio, visual etc for purposes of committing fraud or to misrepresent an individual's identity.
- Do review output of AI applications to make sure it meets Organisation's standards for principles of equity, ethics, and appropriateness.

Monitoring

BSO reserves the right to access and monitor the use of AI applications on any organisation-issued devices or that appears on organisation managed networks to ensure compliant use of these systems. In addition to individual responsibilities listed in this policy, managers are responsible for approving and monitoring AI use within their respective service areas.

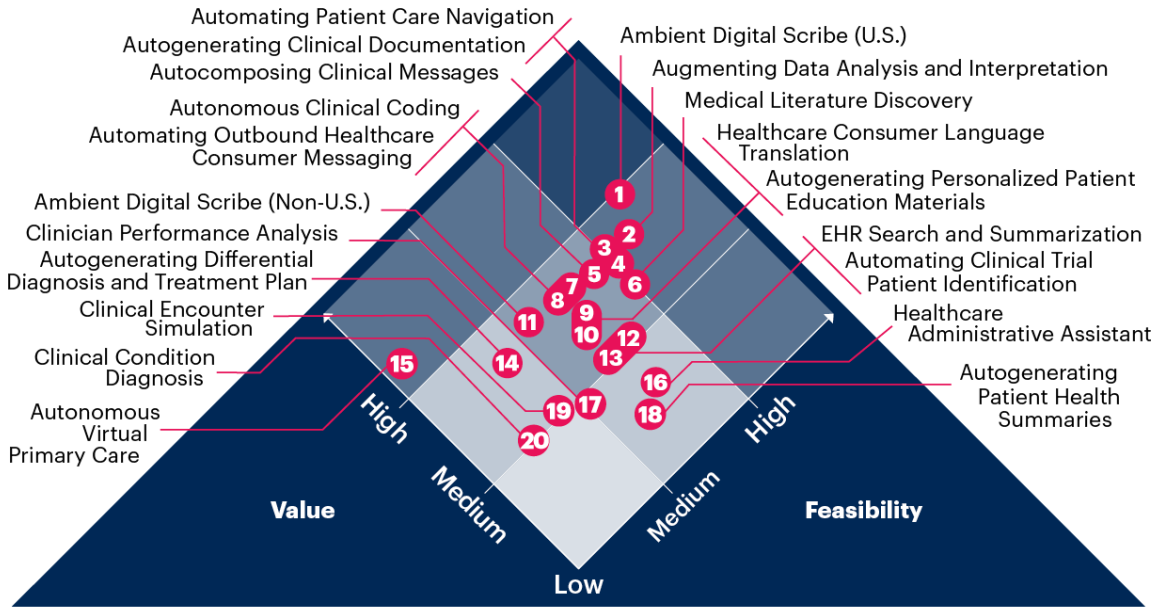
Failure to Comply

Users who fail to comply with any provision of this Policy may be subject to discipline up to and including termination of employment. Violations by contractors may be considered breach of contract and result in removal from assignment. Any AI-related activities which appear to violate applicable legislation will be reported to appropriate authorities.

If monitoring systems and processes detect a possible policy violation or if a User reports a possible policy violation, the suspect event should be processed using appropriate security incident response processes.

Appendix 1 – Use Cases

To better understand the potential of AI, the following examples have been taken from Gartner.



UC San Diego Health Leverages Epic Systems to Autocompose Clinical Messages

Goal

UC San Diego Health (UCSDH) physicians are often responding patient after hours which is contributing to feelings of burnout. It sought to reduce the cognitive and administrative burden on clinicians associated with responding to these messages.

Solution

UCSDH adopted its EHR vendor, Epic Systems,' solution to automate draft responses to "In Basket" messages. Epic is using the Microsoft Azure OpenAI Service to generate the draft reply. An addendum is added to each message generated through the service explaining that the response was autogenerated and reviewed and edited by a clinician prior to sending.

Results

- The solution is generating more comprehensive responses helping to reduce unnecessary appointments
- A study is currently in progress to measure quality improvement outcomes, such as improved patient and clinician experience

Source: The Future is Now: The Power of Generative AI in Healthcare
Source: UCSD Health AI Pilot Program Seeks to Ease Docs' Workload
Source: Microsoft and Epic expand strategic collaboration with integration of Azure OpenAI Service

UC San Diego Health | Epic

Healthcare provider use case

Autocomposing clinician messages	Prism quadrant: Likely wins

Deployment model	Deployment status
Consumer-generative AI embedded in apps	Available in market

Business value

Increase revenue	Increase efficiency
Manage risk	Increase non-financial value

Emory Healthcare Uses Abridge to Reduce Clinician Documentation Time

Goal

Time spent on clinical documentation is a significant contributor to clinician burnout. Emory Healthcare is seeking to reduce clinician documentatic including "pajama time" (after hours documentation).

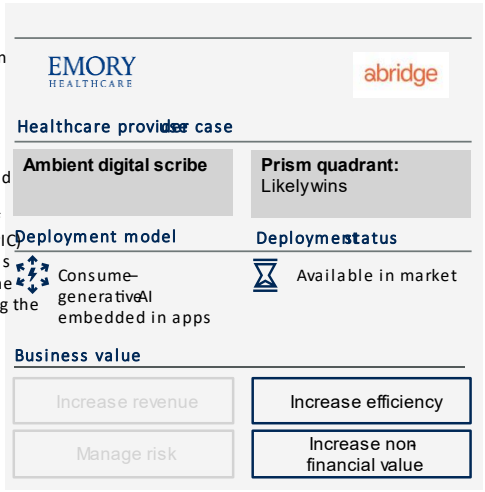
Solution

Abridge's ambient digital scribe solution is in the process of being deployed across the organization. The ambient digital scribe solution automates the documentation of a clinical encounter for clinician review, edit and sign off before uploading it to the relevant fields of the electronic health record (EPIC) through integration using APIs. The solution leverages a series of ML models including LLMs to transcribe the conversation, classify, structure and map the information to standardized ontologies, before summarizing and generating the clinical note.

Results

- Solution being leveraged by over 500 physicians
- Average saving of two hours per day in clinical documentation time

Source: Abridge becomes Epic's First Pal, bringing generative AI to more providers and patients, including those at Emory Healthcare
Source: Emory's Alistair Erskine, M.D., M.B.A., Explains Partnership With Abridge AI Company



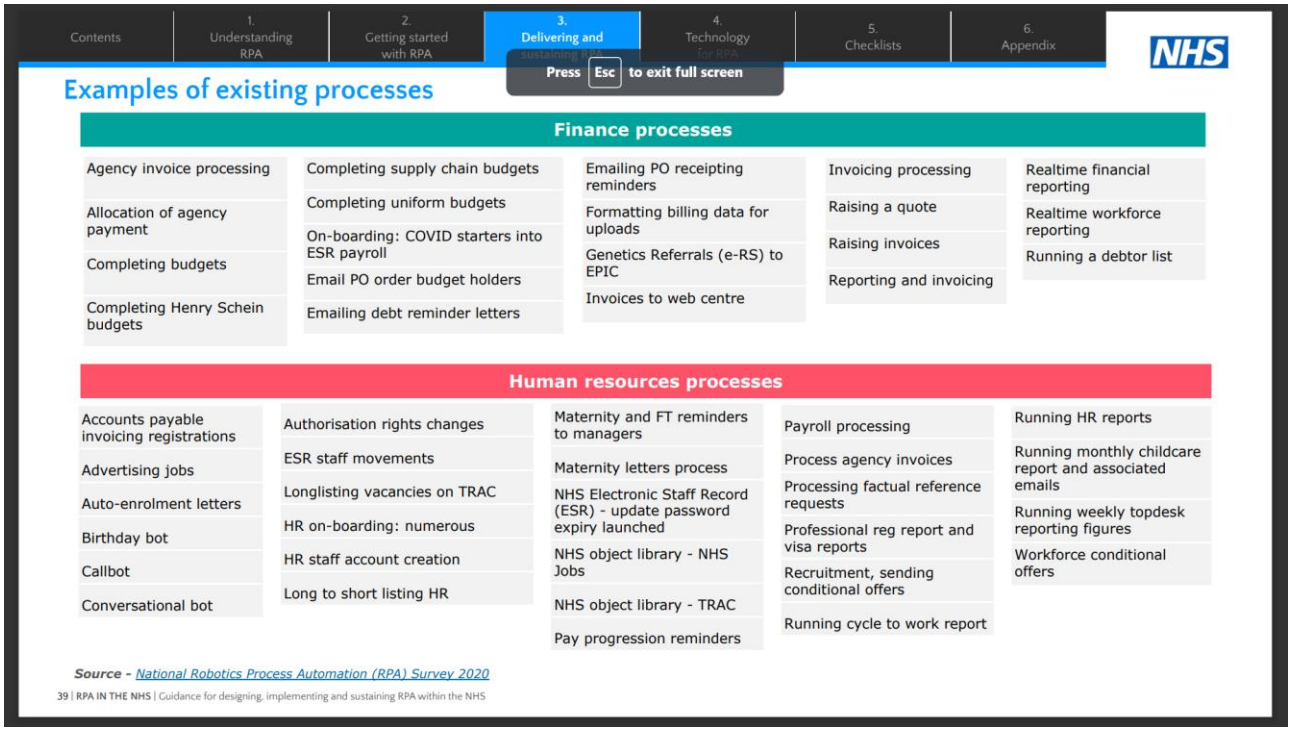
Equip – Oracle Fusion Generative AI capabilities.

Source Oracle AI for Fusion Applications

Table 1: Examples of Oracle's new generative AI capabilities in Fusion Applications

	Assisted Authoring	Suggestions	Summarization
Fusion HCM			
	Employee profile	Survey questions	Performance review summary
	Employee recognition	Competency development tips	Candidate qualification
	Goal creation		
	Job description + requisition		
	Knowledge articles		
Fusion CX			
	Service agent responses	Field service recommendations	Customer engagement summaries
	Knowledge articles		
	Search augmentation		
	Administrator guidance		
Fusion ERP			
	Management reporting narrative		
	Financial reporting narrative		
	Journal entry, reconciliation notes		
	Financial data explanations		
Fusion SCM			
	Item descriptions, attributes		
	Supplier suggestions for negotiations		

Examples of Robotic Process Automation



Appendix 2 – HSCNI Roadmap

Some of the technology on the list below will be made available to BSO and its customers as part of a regional rollout depending on business need and funding.

Available Now

- Bing copilot for work
- AI Training through Microsoft ESI
- NHS AI procurement Frameworks
- NHS AI Virtual Hub - NHS Transformation Directorate (england.nhs.uk)
- AI in imaging: resource collection - NHS Transformation Directorate (england.nhs.uk)

Coming Soon (6 months to 1 year)

- BSO Digital Cloud Team
- Powerapps
- Robotic Process Automation Pilot
- Microsoft Co-pilot test
- NIPACS+ AI Marketplace pathfinder
- NHS AI Regulation Framework

Medium Term (1 to 2 years)

- HSCNI deployment of Open AI or equivalent within HSCNI platform
- Robotic Process Automation rollout
- EPIC AI Integration
- Ambient Listening within Digital Dictation and Voice Recognition
- Fabric Copilot – AI for data analytics

Longer Term (2 years+)

- Oracle Generative AI within Equip
- M365 Copilot