

10th June 2025

To Whom It May Concern

Re: Surgery Intellect (X-on Health and Tortus AI) Compliance with NHS England AVT Requirements

Surgery Intellect (Tortus AI and X-on Health) - Complete Compliance with NHS England AVT Requirements

Executive Summary: Surgery Intellect (X-on Health and Tortus AI) confirms full compliance with all NHS England requirements for Ambient Voice Technology as outlined in the Priority Notification dated 9th June 2025 from Dr Alec Price-Forbes, National Chief Clinical Information Officer. We exceed standards in multiple areas and maintain comprehensive governance oversight across all deployments.

This letter confirms that *Surgery Intellect*—a product of **X-on Health**, powered by **Tortus AI**—fully complies with all NHS standards for Ambient Voice Technology (AVT) solutions. As the contracting entity, **X-on Health** ensures complete alignment with NHS requirements, supported by a strong governance framework focused on clinical safety, data protection, and operational excellence. **Tortus AI**, as the AVT technology provider, meets all necessary regulatory and technical standards required for safe deployment. With robust DPIAs in place, including a comprehensive overarching DPIA, *Surgery Intellect* is now being introduced to the market—delivering advanced, voice-enabled clinical support seamlessly into surgical workflows across all care settings.

Quick glance checklist

Core Platform Assurance Requirements

Requirement	Tortus AI Compliance	X-on Health Compliance	Compliant
DTAC Ready	Full DTAC compliance achieved across all five pillars. ISO 27001 in progress.	DTAC Ready with all five pillars met. ISO 27001 certified. ISO Certification	✓
DSPT	‘Standards Exceeded’ status (ODS: O2G5U) DSPT Report	‘Standards Exceeded’ status (ODS: 8JM42) DSPT Report	✓
Cyber Essentials Plus	Current certification with zero vulnerabilities (8FoldGovernance, Leo CybSec) Cyber Essentials Plus Certification	Current certification (3B Data Security) Cyber Essentials Plus Certification	✓
CREST-approved Pen Testing	Regular CREST-approved testing with zero vulnerabilities Application Retesting Report	Regular CREST-approved testing Penetration Testing Report	✓
Named Clinical Safety Officer	Dr. Dom Pimenta & Nikita Adatia (Named CSOs)	Dr. Imran Khan (Named CSO)	✓
Encryption	AES-256 at rest, TLS 1.2+ in transit, MFA, SSO, RBAC; ISO 27001 in progress	AES-256 at rest, TLS 1.2+ in transit, MFA, SSO, RBAC; ISO 9001, 14001, 22301, 27001, 42001 certified ISO 9001 ISO 14001 ISO 22301	✓

		ISO 27001 ISO 42001	
GDPR Compliance	Full GDPR compliance with UK/EU data sovereignty	Full GDPR compliance with UK/EU data sovereignty	✓
No Unsafe Functionality	Aligned with DCB0129 and ISO 14971 standards	Aligned with DCB0129 and ISO 14971 standards	✓
NHS System Integration	Native integration with Epic; Cerner available site-by-site; EMIS/TPP integration supported via X-on; FHIR R4 & HL7 v2 compliant with write-back.	Direct API integration with EMIS and SystmOne/TPP, including write-back; FHIR R4 & HL7 v2 compliant; integration underpins Tortus support.	✓
Translation Accuracy Responsibility	No language translation; full transcription responsibility	No language translation; full transcription responsibility	✓

Enhanced Requirements

Requirement	Tortus AI Compliance	X-on Health Compliance	Compliant
Medical Device Classification	MHRA Class 1 registered; Class 2a application submitted MHRA Registration Certificate	Supports Tortus AI's medical device registration	✓
Data Protection	Automatic deletion of patient session data after 24 hour	Automatic deletion of patient session data after 24 hour	✓
System Integration	Native integration with Epic; Cerner available site-by-site; EMIS/TPP integration supported via X-on; FHIR R4 & HL7 v2 compliant with write-back.	Direct API integration with EMIS and SystmOne/TPP, including write-back; FHIR R4 & HL7 v2 compliant; integration underpins Tortus support.	✓

Clinical & Operational Threshold Benefits

Requirement	Tortus AI Compliance	X-on Health Compliance	Compliant
Evidence of NHS Clinical Validation	Validated via NHS clinical studies: 17,000 patient study. Early data from our Phase IV study with 473 patient observations shows a 16.9% increase in direct patient care time, while our real-world evaluation spanning 4,890 consultations has achieved a 99% acceptance rate. Clinical satisfaction metrics show that 97% of clinicians report ability to give full attention to patients, compared to just 67% at baseline, and 82% of clinicians rate their experience as better than previous clinics without AVT.	Supports deployments in the NHS via joint solution.	✓
Economic Justification and Workforce impact	Our economic modeling shows a return on investment of 30-40x through multiple value streams. In Emergency Departments, early data suggests 20% productivity improvements through the largest trial of AVT technology in UK ED settings, enabling increased patient throughput and reduced waiting times..	Supports joint ROI in workforce efficiency data.	✓

1. Core Platform Assurance Requirements

✓ **NHS Requirement:** *"Digital Technology Assessment Criteria (DTAC), Data Security and Protection Toolkit (DSPT), Cyber Essentials Plus, CREST-approved pen testing"*

TORTUS Compliance:

TORTUS has achieved full DTAC compliance, having successfully passed all five pillars: clinical safety, data protection, technical security, interoperability, and usability. Our DSPT submission has achieved "Standards Exceeded" status (ODS Code: O2G5U), demonstrating our commitment to exceptional data security practices beyond minimum requirements. We maintain current Cyber Essentials Plus certification alongside regular CREST-approved penetration testing, with our latest assessment conducted by 8FoldGovernance and Leo CybSec reporting zero vulnerabilities. Certificate available [here](#).

X-on Compliance:

X-on Health has completed full DTAC ready status, having successfully covered all five of the Pillars. Our DSPT submission was fully audited and achieved the "Standards Exceeded" status (ODS Code: 8JM42), which demonstrates our commitment to exceptional data security practices beyond the minimum required. We maintain a current Cyber Essentials Plus certificate alongside our regular Crest approved penetration testing with our latest assessment conducted by 3B Data Security. Certificate [here](#).

✓ **NHS Requirement:** *"Data Protection Requirements as set by ICO - Local ICB / Trust governance approval including DPIA completion"*

TORTUS Compliance:

TORTUS maintains a rigorous approval process, obtaining full ICB approvals before any deployment. We are approved or in process with the majority of ICBs across England and maintain a comprehensive Data Protection Impact Assessment that is continuously updated to reflect evolving system capabilities, deployment contexts, and regulatory requirements. Our DPIA is aligned with NHS DSPT, DCB0129, and GDPR guidance, outlining detailed data flows, processing purposes, access controls, retention policies, and risk mitigations. This documentation is shared with NHS partners as part of governance onboarding. Our solution fully complies with ICO requirements, incorporating principles of data protection by design and default, with all processing activities subject to internal and external review.

X-on Health Compliance:

X-on Health maintains a rigorous approval process, obtaining full ICB approvals before any deployment. We are approved or in process with the majority of ICBs across England and maintain a comprehensive Data Protection Impact Assessment that is continuously updated to reflect evolving system capabilities,

deployment contexts, and regulatory requirements. Our DPIA is aligned with NHS DSPT, DCB0129, and GDPR guidance, outlining detailed data flows, processing purposes, access controls, retention policies, and risk mitigations. This documentation is shared with NHS partners as part of governance onboarding. Our solution fully complies with ICO requirements, incorporating principles of data protection by design and default, with all processing activities subject to internal and external review. .

✓ **NHS Requirement: "Clinical Safety Officer(s) named and accountable"**

TORTUS Compliance:

Dr Dom Pimenta MBBS MRCP BSc (Hons) (CEO) and Nikita Adatia MPharm (First Class Hons), PgDip Pharmacy Practice, CEPIP, PharmIP serve as designated Clinical Safety Officers, ensuring direct executive accountability for all clinical safety aspects. Both officers maintain current DCB0160 certification and oversee our clinical safety management system including quarterly reviews and incident response protocols aligned with NHS Digital clinical risk management standards.

X-on Health Compliance:

Dr Imran Khan B.Eng PhD MBBS MRCP is our designated Clinical Safety Officer and consultant, ensuring direct executive accountability for all clinical safety aspects. Our officer maintains current DCB0160 certification and oversees our clinical safety management system including quarterly reviews and incident response protocols aligned with NHS Digital clinical risk management standards.

✓ **NHS Requirement: "End-to-end encryption and GDPR compliance"**

TORTUS Compliance:

Comprehensive encryption protocols implemented using AES-256 standards for data at rest and TLS 1.2 or higher for data in transit. Full GDPR compliance framework established with UK/EU data sovereignty - all data is processed and hosted within the UK or EEA with no cross-border transfers without explicit documented exceptions. We enforce multi-factor authentication (MFA) and single sign-on (SSO) with role-based access control (RBAC) for all sensitive functions. Patient data is never stored remotely; local device/browser storage is ephemeral and auto-deleted after logout or within 24 hours. Our data protection by design approach includes strong minimisation principles, redaction before processing, and full transparency in data handling practices. ISO 27001 certification is currently in progress to further strengthen our security posture.

X-on Health Compliance:

Comprehensive encryption protocols implemented using AES-256 standards for data at rest and TLS 1.2 or higher for data in transit. Full GDPR compliance

framework established with UK/EU data sovereignty - all data is processed and hosted within the UK or EEA with no cross-border transfers without explicit documented exceptions. We enforce multi-factor authentication (MFA) and single sign-on (SSO) with role-based access control (RBAC) for all sensitive functions. Patient data is never stored remotely; local device/browser storage is ephemeral and auto-deleted after logout or within 24 hours. Our data protection by design approach includes strong minimisation principles, redaction before processing, and full transparency in data handling practices. We are certified with ISO 9001, ISO 14001, ISO 22301, ISO 27001 and ISO 42001.

✓ **NHS Requirement: "No unsafe functionality e.g. prompt injection access"**

TORTUS Compliance:

Our system architecture is built on a principle of clinical safety by design, preventing prompt injection through multiple security layers. Importantly, TORTUS does not provide any chat interface or direct user interaction with AI models. All interactions with AI components are mediated through structured, predefined workflows that are clinically validated and context-specific. The platform enforces hard-coded input controls that sanitize and restrict all user inputs, with no ability to issue raw prompts or bypass embedded safety logic. Our verification and validation protocols are aligned with DCB0129 and ISO 14971 standards to monitor and mitigate AI-related clinical risks. This secure-by-design architecture ensures that prompt injection, adversarial manipulation, or misuse of generative features is technically impossible in production environments.

X-on Compliance:

Our system architecture is built on a principle of clinical safety by design, preventing prompt injection through multiple security layers. All interactions with AI components are mediated through structured, predefined workflows that are clinically validated and context-specific.. Our verification and validation protocols are aligned with DCB0129. This secure-by-design architecture ensures that prompt injection, adversarial manipulation, or misuse of generative features is technically impossible in production environments.

✓ **NHS Requirement: "Appropriate NHS clinical system integration (API or FHIR/HL7 compliance and write-back capability)"**

TORTUS Compliance:

TORTUS provides comprehensive NHS clinical system integration with native support for FHIR R4 and HL7 v2 standards. We have implemented direct native integration with Epic systems, ensuring seamless operation within this major EHR platform. For EMIS and SystmOne/TPP, we partner with X-On Health to enable full data write-back functionality through secure, standards-based APIs underpinned by OAuth 2.0 authentication and TLS 1.2+ encryption. Cerner integration is available on a site-by-site basis, tailored to each Trust's specific

requirements. Our modular architecture allows deployment with or without EPR integration, depending on local policy and readiness, with all integrations co-developed with trust IT teams and validated in sandbox environments before deployment. Custom integrations are also supported to accommodate unique clinical environments and workflows.

✓ **NHS Requirement:** *"The responsibility for translation accuracy remains with the AVT supplier"*

TORTUS Compliance:

TORTUS AI focuses exclusively on clinical documentation in English. We do not provide language translation services, eliminating this risk vector while maintaining full responsibility for transcription accuracy.

X-on Compliance:

X-on focuses exclusively on clinical documentation in English. We do not provide language translation services, eliminating this risk vector while maintaining full responsibility for transcription accuracy.

2. Enhanced Requirements

✓ **NHS Requirement:** *"Medical Device Classification – All AVT solutions that undertake summarisation require, at least, MHRA Class 1 medical device status. Companies must NOT extend system capabilities to produce generative diagnoses, management plans, or other medical referrals and calculations without seeking at least MHRA Class 2a approval."*

TORTUS Compliance:

MHRA Class 1 medical device registration confirmed ([PARD reference](#)). Additionally, we have proactively submitted for Class 2a certification with our Notified Body, anticipated completion September 2025, demonstrating our commitment to highest regulatory standards. Our system strictly limits functionality to transcription and summarization, with no capability for generating diagnoses, management plans, or medical referrals.

✓ **NHS Requirement:** *"Data Protection – Safeguarding Patient Information is paramount. Patient data from clinical sessions (e.g. immediate inference) should be automatically deleted unless legally or operationally required, in line with UK GDPR and DPA 2018 principles on data minimisation and storage limitation."*

TORTUS Compliance:

Our system automatically deletes all patient session data after 24 hours, exceeding data minimisation requirements. This functionality is built into our core architecture, ensuring consistent application across all deployments. Clear

audit trails maintained for all data processing activities with detailed retention schedules developed in consultation with Information Governance teams.

✓ **NHS Requirement:** *"System integration – Ensure appropriate integration with your IT infrastructure, systems and workflows. For example, in most general practice and hospital settings, AVT solutions will require integration with the principal electronic record system."*

TORTUS Compliance:

TORTUS provides native integration into Epic systems, ensuring seamless operation within this major EHR platform. We offer supported integration with EMIS and SystmOne/TPP through our partnership with X-On Health, designed for optimal interoperability. Cerner integration is available on a site-by-site basis, tailored to each Trust's specific requirements. Custom integrations are also supported to accommodate unique clinical environments and workflows. All integrations maintain full FHIR/HL7 compliance with comprehensive write-back capabilities.

3. Clinical and Operational Benefits Thresholds

✓ **NHS Requirement:** *"Evidence of real-world clinical validation of benefits in the NHS care setting proposed (e.g. enhancing clinical efficiency and workflow, reducing administrative burden; improving patient care by increasing face to face time with patients; improving accuracy of documentation; improving data quality and capture of structured data recorded in electronic patient record systems)"*

TORTUS Compliance:

TORTUS has established comprehensive real-world NHS validation through extensive clinical studies and deployments. We are about to publish a landmark 17,000 patient real-world study spanning every major care setting in the NHS, including primary care, secondary care, emergency departments, and mental health services. Early data from our Phase IV study with 473 patient observations shows a 16.9% increase in direct patient care time, while our real-world evaluation spanning 4,890 consultations has achieved a 99% acceptance rate. Clinical satisfaction metrics show that 97% of clinicians report ability to give full attention to patients, compared to just 67% at baseline, and 82% of clinicians rate their experience as better than previous clinics without AVT. Additionally, we have proven our capability to capture structured data at all required levels, significantly enhancing EPR data quality.

✓ **NHS Requirement:** *"Clear economic justification and workforce impact"*

TORTUS Compliance:

TORTUS has demonstrated clear economic justification through early productivity data and comprehensive workforce impact assessments. Our economic modeling shows a return on investment of 30-40x through multiple value streams. In

Emergency Departments, early data suggests 20% productivity improvements through the largest trial of AVT technology in UK ED settings, enabling increased patient throughput and reduced waiting times. Similar efficiency gains in outpatient departments allow clinicians to see more patients within existing clinic capacity. Technology consolidation benefits arise from replacing multiple documentation methods with a single, integrated solution, reducing overall IT complexity and training requirements. The workforce impact extends beyond direct time savings, with clinicians reporting reduced administrative burden, improved work-life balance through decreased documentation completed outside clinical hours, and enhanced job satisfaction. These combined benefits create a compelling economic case for AVT adoption across all NHS care settings.

Commitment to Ongoing Compliance

Surgery Intellect—a product of **X-on Health**, powered by **Tortus AI**—maintains continuous compliance through regular engagement with ICBs, quarterly clinical safety reviews, and proactive regulatory submissions. As the contracting entity, X-on Health ensures that our governance framework not only meets but exceeds NHS requirements, setting a new benchmark for Ambient Voice Technology (AVT) deployment in clinical environments.

We welcome further scrutiny and remain fully available for audit or clarification regarding our compliance framework. Our team is committed to supporting NHS England's vision for safe, effective AVT adoption across all care settings.

Please refer to the following sections for supporting documentation and additional details. If you require further information or would like to discuss any aspect of our compliance framework, do not hesitate to contact us directly using the information provided at the end of this document.

Yours sincerely,
Dr Dom Pimenta MBBS MRCP BSc
(Hons) Chief Executive Officer
TORTUS AI
Email: commercial@tortus.ai

Julian Coe
Managing Direction
X-on Health
Email: