General Information

	Description	Response	For internal Camden use - questions / follow up required
Supplier Information	Name of supplier:	Central and North East London NHS Foundation Trust	
	Contact (name / contact):	Alasdair Tudhope	
	Contract commencement date:	1st July 2025	
	Contract end date:	30th June 2028	
Service offering	Please provide a brief description of the system or service being provisioned. Include the names of any specific products or services being provided.	The provision of integrated sexual health services with North Central London (NCL)	
	Is the system or service hosted on Council premises, or is it a hosted or cloud solution? If the latter, please provide details of the hosting provider and the location(s) where all data will be held.	The majority of reporting will come from our clinical EPR, Cellma. This system has been in situ across all our clinics since 2014 and has links to pathology, pharmacy and radiology. Private hosted cloud service provider Rackspace. Private Cloud datacenters are both UK based within LON3 & LON5. https://www.rackspace.com/en-gb/about/data-centers	
	If cloud hosted how would you describe the service using industry recognised hosting terms (e.g SaaS, PaaS etc)	IaaS which include OS level security patching	
	Based on current understanding, and accepting this may change after further analysis, please provide a list of anticipated interfaces with other systems	No interfaces to Camden systems	
Key info	Do you require access to Camden's internal systems via a VPN into Camden's internal network? (Note, if so you will also need to fill out a Code of Connection)	No, we do not need to access this.	
	What categories of data does this product or service process (e.g. business: employee; Customer Information; Residents)	Cellma is our clinical system that will hold service user data.	
	Does the system process 'Personal Data'?	Yes	
	Does the system process 'Sensitive Personal Data'?	Yes	
	Does the system process payment card information or interface with a system which does, for e.g. payment card gateway?	No	
	What are your key SLAs for availability and service management	The entire server infrastructure, including network endpoints (switches, routers, WAN, HSCN), is monitored 24/7 by a dedicated service center.	

	If your solution includes Disaster Recovery, what is the Recovery Point Objective (RTO) and Recovery Time Objective (RPO)	Our disaster recovery solution is designed to ensure business continuity and minimise data loss through a robust hybrid cloud infrastructure. The Recovery Time Objective (RTO), which defines the maximum acceptable time to restore services after a disruption, is optimized through the use of a virtualised server environment and 24/7 monitoring. With this setup, any outages or critical issues are detected immediately, and incident resolution workflows are initiated, ensuring rapid recovery. The combination of our infrastructure and continuous monitoring allows us to maintain an RTO that ensures minimal downtime and swift service restoration. The Recovery Point Objective (RPO), which determines the maximum acceptable amount of data loss measured in time, is minimized through regular offline data backups and redundancy in the cloud infrastructure. This ensures that, in the event of a disaster, data can be restored up to the most recent backup, keeping data loss to a minimum. Our disaster recovery setup is aligned with best practices to meet both RTO and RPO targets that support the critical nature of healthcare services, prioritizing minimal disruption and maintaining service integrity.	

For completion by Camden		
Internal Information	Date review was completed	
	Completed by:	
	System / Service Name:	
	Primary Camden IT Contact:	
	Project Name:	
	Project Manager (name / contact):	

Requested Documentation

Camden requests that you provide documentation to assist with Camden's assessment of the solution.
Please attach these documents in an email to Camden and reference their name here, or provide URLs to the documentation in the tables below.

Some of this may not be relevant to your particular service, the SCA caters for a wide range of suppliers and services. Just ignore those elements.
If you don't have all the information (the list below is extensive), supply what you can and allow time for further discussions with the security team.
You can provide multiple documents against each topic, or the same document can be used across multiple topics. Just make it clear where the relevant information can be found.

Solution Architecture

Topic	Contents expected	Supplied (Y/N or N/A)	Document(s) Name(s) / URL(s)	Document section(s) (if covered as part of a larger document and not obvious where to find the content)	Comments	For internal Camden use - questions / follow up required
Technology architecture	A high level description of the architecture of the provided service, covering the network, compute and storage infrastructure used to deliver the service, plus the application architecture.	N/A	We are able to provide a walkthrough; however, please note that due to cybersecurity protocols, these documents cannot be shared			
Security architecture	Covers the security controls at the various layers, including: compute layer (e.g. device hardening, anti virus); network layer (e.g firewalls, encryption, IDS), storage layer (e.g. encryption at rest); application layer (e.g configuration hardening); service management layer (e.g. log management, monitoring and alerting tools). If the environment is multi tenanted, the document should cover how secure tenancy segregation is achieved.	N/A	We are able to provide a walkthrough; however, please note that due to cybersecurity protocols, these documents cannot be shared			
Disaster recovery and resilience architecture	Covers how backup, resilience and disaster recovery are architected into the solution, includes details of SLAs, RPO and RTO and how they are achieved, and the support processes for managing outage and failover.	N/A	We are able to provide a walkthrough; however, please note that due to cybersecurity protocols, these documents cannot be shared			
Integrations and interfaces	To the extent currently known, describe the integrations / interfaces to other systems and how these are secured and authenticated. Also how different categories of users (citizens, Camden staff, supplier and third party support and admins) can login and authenticate. Camden has some preferred approaches which will be supplied to you seperately.	N/A	We are able to provide a walkthrough; however, please note that due to cybersecurity protocols, these documents cannot be shared			
Service Architecture	Describe the service management tooling used to keep the service secure and operational. This should include how the service is monitored, and how logs are managed, protected and reviewed for alerts and security incidents.	N/A	We are able to provide a walkthrough; however, please note that due to cybersecurity protocols, these documents cannot be shared			
Service Description	Details of the support wrap included in the service, including any applicable SLAs, the division of responsibilities between the supplier and Camden, and any relevant support processes.	N/A	We are able to provide a walkthrough; however, please note that due to cybersecurity protocols, these documents cannot be shared			
Other	Any relevant other documents that help to clarify the service offering or how it is delivered, secured, or service managed	N/A	We are able to provide a walkthrough; however, please note that due to cybersecurity protocols, these documents cannot be shared			

Certifications and Standards

If you, your subcontractors or hosting providers hold any relevant security certifications or meet industry recognised standards such as ISO 27001, Cyber Security Plus, please reference them here.
Please include any data centre or hosting specific certifications standards (such as ISO, EN or Uptime Institute), especially anything relating to physical security, energy efficiency and sustainability

Standard or Certifications	Scope (who or what does this apply to)	Document(s) Name(s) / URL(s)	Comments	Certificate Expiry Date	For internal Camden use - questions / follow up required
	Rackspace please follow link to certifications	Governance, Risk, & Compliance Services | Rackspa			
	CNWL	NHS DSPT (Cyber Essential+)			
	Riomed (Cellma supplier)	RioMed Contact us			

Other Documents

These could include other policy documents you have created to align with ISO27001, ITIL or other industry standards, such as change management or encryption key management policies
If there are polices you hold but cannot share, please list them here and explain why they cannot be shared

Topic	Contents expected	Supplied (Y/N or N/A)	Document(s) Name(s) / URL(s)	Document section(s) (if covered as part of a larger document)	Comments	For internal Camden use - questions / follow up required

For Camden Security Team only

Comments against docs supplied for DPIA

Document	For internal Camden use - questions / follow up required

Additional Questions

These are areas where we require specific clarification.
These may be covered in other submitted documentation, if so, just reference the documents in your response rather than copying and pasting sections from them (including the section where the information is if not obvious).

Not all questions will be relevant, as this questionnaire covers a wide range of services and providers. Just put N/A if the question is not applicable.
For guidance, for some of the questions we have provided a minimum standard expected in the response. If the minimum standard is not met, this will require further discussion.
If you don't have all the information (the list below is extensive) supply what you can and allow time for further discussions with the security team.

This questionnaire is Camden's own, but is structured in line with and loosely based on the Cloud Security Alliance CAIQ 4.1 questionnaire
Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 | CSA (cloudsecurityalliance.org)

Camden Question ID	Topic	Camden question	Minimum standard expected	Customer response and Evidence	For internal Camden use - questions / follow up required
1.1	Application and Interface Security	How is security built into your Software Development Lifecyle (SDLC)? If you follow any applicable industry standards, please describe this here.	Evidence that security is considered during the SDLC and secure code is delivered by following a robust methodology, including how you test for vulnerabilities during testing.	N/A	
1.2	Application and Interface Security	Describe your vulnerability management strategy for the application and frequency.	Description of SLAs and action plan on the vulnerability remediation. Camden expects all critical vulnerabilities to be remediated within 2 days and High's within 4 working days unless mitigating controls are in place.	CNWL's vulnerability management strategy involves conducting annual penetration testing on all systems, with results reported directly to the SIRO (Senior Information Risk Owner). Any vulnerabilities identified are assessed based on risk, and mitigation actions are taken within agreed timescales according to the severity of the risk. This approach ensures that any potential security gaps are promptly addressed to maintain the integrity and security of the systems. Additionally, CNWL's compliance with ISO27001 and ISO27002 standards, as well as the use of an Information Asset (IA) register, ensures that all assets are tracked and monitored for vulnerabilities. Regular updates to the IA register, combined with risk mitigation by asset owners, further strengthens the organisation's proactive approach to managing security risks.	
1.3	Application and Interface Security	Does the software have any 3rd party dependencies?	Describe how you ensure your suppliers adhere to security best practices.	All suppliers must possess ISO/IEC 27001 certification to provide services to CNWL. This certification is a globally recognized standard for information security management systems (ISMS). It ensures that suppliers have implemented robust security measures to protect sensitive information, manage risks effectively, and comply with legal and regulatory requirements. By requiring this certification, CNWL ensures that all suppliers adhere to high standards of cybersecurity, thereby safeguarding the integrity and confidentiality of data.	
2.1	Audit Assurance and Compliance	Do you conduct Network/application penetration tests of any infrastructure providing the Camden service at least annually?	Camden expects independent 3rd party assessment at least once a year, (with evidence of the results shared. Executive summary only)	Yes, we conduct annual network and application penetration tests on all infrastructure. The results of these tests are reported to the SIRO (Senior Information Risk Owner), and any identified vulnerabilities are addressed within agreed timescales based on the level of assessed risk. This ensures ongoing security and compliance with industry standards, maintaining the integrity of the infrastructure.	
3.1	Business Continuity Management	Describe the business continuity and disaster recovery plans for the Camden-provided service.	These need to be in place and subject to periodic testing at least once a year, at planned intervals or upon significant changes to ensure continuity and test effectiveness.	CNWL has established comprehensive business continuity and disaster recovery plans, ensuring resilience and uninterrupted service delivery in the event of disruptions. Key elements of our strategy include: Extensive Disaster Recovery Infrastructure: Our hybrid cloud design incorporates advanced disaster recovery options for all critical Information Management & Technology (IM&T) infrastructure. This includes the removal of single points of failure and fully virtualised server infrastructure, ensuring robust backup systems are in place. Regular Testing and Updates: Disaster recovery plans are regularly tested and updated to align with current best practices and to ensure their effectiveness. This proactive approach allows us to adapt to any changes in the operational environment or technological advancements. 24/7 Service Support: We provide continuous support through a 24/7 service desk, which ensures that any incidents or requests are addressed promptly. This capability is crucial for maintaining operational continuity, particularly in high-demand settings. Automated Processes: Our ICT service management processes leverage automation to enhance service delivery and response times. For instance, operating system patching is automated and aligned with Microsoft's monthly vulnerability releases, reducing risks associated with outdated systems. Incident Management and Reporting: Incidents are logged and managed through our internal database, which enables efficient tracking and management of all ICT assets. This system is integral to our lifecycle management process, ensuring that any potential risks are identified and mitigated effectively. Engagement with External Suppliers: All external suppliers are required to adhere to the National Cyber Security Centre principles and standards, ensuring that they contribute to the overall resilience of the service. Compliance is monitored through regular reporting and performance reviews.	
4.1	Data management	What is your backup mechanism and how long are your backups kept for?	Camden expects backups to be kept for at least a month	CNWL employs a comprehensive and systematic backup mechanism designed to ensure the integrity and availability of critical data across all services. We conduct regular offline backups of all essential systems, utilising cloud technologies that provide scalable and secure storage solutions. This approach not only enhances our disaster recovery capabilities but also aligns with industry best practices, ensuring that data can be restored efficiently in the event of an incident. Backups are retained for a predefined period, which is established in accordance with regulatory requirements and organizational policies. While the exact retention duration may vary depending on the type of data, we are committed to complying with relevant legislation, including GDPR, which mandates appropriate data management and retention practices. This ensures that data is kept as long as necessary for operational and legal purposes, while also safeguarding against unnecessary data retention.	

4.2	Data management	Are backup and redundancy mechanisms tested at least every six months to a year?	That you do conduct such tests at least annually (documented policy)	Yes, CNWL conducts regular testing of backup and redundancy mechanisms to ensure their effectiveness and reliability.	
4.3	Data management	Does Camden have full access to all its data held by you on our behalf?	We would expect to easily be able to access all our data on demand via APIs and/or database/file connectivity, so that we can use it for other purposes.	No - Camden does not have access to our data. These are confidential medical records	
4.4	Data management	On contract termination, is there a process whereby Camden can extract all its data in an industry standard format (e.g. CSV)?	We would expect a suitable process and format to exist.	No data can be provided as these are confidential medical records	
5.1	Change management	Do you have policies and procedures for change management, that are followed both by you and third parties working on the system.	We are expecting evidence that change is applied in a controlled way, with security impact assessment, in collaboration with Camden, and the ability to roll back changes. We would expect the same standards to be applied to any third parties working on the service.	We have a formal ITIL v4 change management process, there is no connectivity to Camden service / networks so Camden are not involved in changes	
5.2	Change Management	Are mechanisms in place to ensure that all debugging and test code elements, configurations and accounts are removed from released software versions?	We would like confirmation of how this is done as part of your acceptance into the service process. (evidenced through documented policy)	N/A	
6.1	GDPR Compliance	Describe your approach to GDPR compliance and any controls in place. This includes 1. How the system meets the GDPR article 17 "right to be forgotten" requirement		We adhere to the accountability principles outlined in the UK GDPR, ensuring that personal data is managed appropriately and in accordance with legal requirements. Our comprehensive Information Governance (IG) policy framework guides our compliance efforts, encompassing robust operational procedures and processes to address data protection obligations effectively. To meet the "right to be forgotten" requirement specified in Article 17 of the GDPR, we have established a systematic process for handling requests from individuals wishing to erase their personal data. Patients are informed of their rights regarding data access and erasure through clear privacy notices that explain the data collection, use, and retention processes. These notices are strategically placed and easily accessible to ensure that patients understand how their personal data is handled. When a request for erasure is received, our designated Subject Access Request Coordinators (SARCs) are trained to assess and process these requests in line with our Access to Health Records Procedures. Each request is evaluated to determine whether the legal grounds for erasure are met, and if so, appropriate steps are taken to remove the individual's data from our systems. We maintain an internal database to log such requests, ensuring accountability and tracking the status of each case. Additionally, we implement data retention schedules that dictate how long personal data is retained before it is securely deleted. This ensures that we do not hold data longer than necessary, which aligns with the principles of data minimisation and limited retention. Our central IG Team conducts regular reviews and audits to ensure compliance with these practices, further supporting our commitment to GDPR obligations.	
6.2	GDPR Compliance	How does the system meet GDPR article 15 - the customer has the right to see data held about them in a system		To facilitate this right of access, we have implemented a clear and streamlined process for handling Subject Access Requests (SARs). Each service within our organisation has designated SAR Coordinators (SARCs) who are specifically trained in the legal and procedural requirements for processing such requests. These coordinators guide patients through the process, ensuring that they understand their rights and the steps involved in accessing their data. When a patient submits a SAR, the request is logged in our internal database, and the SARCs take prompt action to gather the requested information. We adhere to statutory timelines, ensuring that responses to requests are provided within one month, as mandated by the GDPR. In cases where the request is complex or involves a large volume of data, we may extend this timeframe, but we will communicate any delays to the patient promptly. To enhance transparency and accessibility, we provide clear privacy notices that outline how patients can exercise their right to access their personal data. These notices are readily available and written in plain language, making it easier for individuals to understand how to submit a request and what information they can expect to receive.	
6.3	GDPR Compliance	How does the system enable data retention policies to be configured so that data can be removed as soon as there is no valid reason for us to continue holding that data?		We adhere to the Record Management Code of Practice for Health and Social Care 2021, which outlines our obligations regarding the retention and disposal of records. Each type of data collected and processed is categorised based on its purpose, and retention schedules are established accordingly. These schedules dictate how long different types of records are kept, ensuring that data is not retained beyond its useful life. Our systems, including the Calma clinical IT platform, enable the configuration of automated data retention policies. This allows for the systematic review and removal of data that no longer has a valid reason for being held. The automated processes ensure that data is flagged for review and deletion when it reaches the end of its retention period. This reduces the risk of human error and enhances compliance with data protection regulations.	
7.1	Data Security	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Camden's preference is that non production environments should only use dummy data for anything sensitive. If it is necessary for any reason for production data to be used in non-production environments, then these must be managed to the same security standards as the production environment.	This is patient Identifiable Data and is only used for direct Healthcare purposes.	
7.2	Data Security	When Camden exits the service arrangement, will you be able to securely sanitize and if appropriate securely dispose of all resources used to supply the service?	This is required (Destruction/ sanitisation certificate is required within 15 days of contract termination)	No, medical records are retained in line with current legislation/guidance	

7.3	Data Security	How do you prevent, detect, and quickly recover from cyber-attacks on your live data (on servers, PaaS etc)	What measures do you have in place for detecting and preventing potential ransomware attacks within your environment?	At CNWL, we have implemented a comprehensive cybersecurity strategy to prevent, detect, and quickly recover from cyber-attacks on our live data across servers and Platform as a Service (PaaS) environments. Our approach is guided by the principles outlined by the National Cyber Security Centre and includes several key elements: 1. Preventive Measures: Robust Access Controls: We implement strict access controls to ensure that only authorised personnel can access sensitive data. This includes role-based access management and the use of smart cards to authenticate users. Regular Security Updates and Patch Management: Our systems undergo regular updates to address vulnerabilities. We automate operating system patching in line with Microsoft's monthly vulnerability releases to mitigate risks. Security Awareness Training: All staff undergo mandatory cybersecurity training, which covers best practices for data protection, recognising phishing attempts, and understanding the importance of safeguarding sensitive information. 2. Detection Mechanisms: Monitoring and Threat Detection: We employ advanced threat detection tools that monitor our systems in real-time for unusual activity. This includes the use of technologies such as Bit Sight, PDNS, and ATP to identify and respond to potential threats proactively. Incident Reporting Protocols: Our Incident Management system (ServiceNow) allows for the swift reporting and tracking of any security incidents or anomalies. This ensures that potential threats are identified and escalated quickly for further investigation. 3. Response and Recovery Plans: Incident Response Team: We have established a dedicated Incident Response Team that is trained to respond to cybersecurity incidents swiftly. This team conducts investigations, implements containment strategies, and coordinates communication with affected parties. Disaster Recovery and Business Continuity Planning: Our disaster recovery plans include regular backups of critical data, which are stored securely offsite to ensure data integrity and availability. We test our backup and recovery processes at least annually to validate their effectiveness and ensure that we can restore data quickly in the event of an attack. Post-Incident Analysis: Following any cybersecurity incident, we conduct thorough post-incident reviews to identify lessons learned and improve our defences. This feedback loop allows us	
7.4	Data Security	As a result of a successful Ransomware attack, what measures do you have in place to recover deleted or encrypted backup data?	We would expect backups to be protected from ransomware attacks by being suitably segregated from the live environment so that a ransomware attack from a compromised server cannot reach them. This would typically mean that backups are performed at the hypervisor level in a way that is inaccessible to the guest VMs, with additional controls implemented where available such as specialised authentication checks when accessing the backup files (such as a PIN or MFA), alerts if backup files are changed, a method of recovering recently deleted backups, and/or immutable storage.	There is an air gap between production and backup storage. An air gap is a security measure that physically isolates the backup storage from the production environment. This means that the backup storage is not directly connected to the production network, preventing any potential cyber threats from spreading from the production environment to the backup storage.	
7.5	Data Security	How do you ensure that Data changes are logged?"	This would typically be a change log showing old value, new value, date and time of change, and who made the changes.	Logs are retained in AlienVault for analysis when required.	
7.6	Data Security	Does the application have any Data Loss Prevention capabilities to prevent inappropriate sharing of data?	As well as traditional DLP capabilities deployed estate-wide, we are looking for controls or policies such as conditional downloads dependent on user role, device type/location, and prevention of uploads of sensitive data to unauthorized cloud services such as email or cloud storage.	Controls are in place that prevent the download of data to any portable storage devices, Firewall rules are in place to ensure access to non-approve file storage is restricted.	
8.1	Physical Security	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	This is required - you do not need to go into full details if the solution is hosted by a recognised industry cloud provider.	As per Rackspace URL :- https://www.rackspace.com/en-gb/about/data-centers	
8.2	Physical Security	Do you restrict physical access to information assets and functions by users and support personnel?	We would expect that only authorised personnel would have access to areas where the infrastructure used to supply the Camden service is physically held.	Yes - Authorised Rackspace personnel access only	
9.1	Encryption & Key management	Do you encrypt data in transit either **internally or externally** using TLS 1.2 and above	Camden requires all data in transit to be encrypted , regardless of sensitivity.	All data is encrypted in transit via HTTPS connectivity	
9.2	Encryption and Key Management	Is data encrypted at rest (including backup data)?	We would expect this for all sensitive data, wherever held, and for whatever purpose.	All data is encrypted at rest, including backup data. This encryption is part of our comprehensive Information Security Policies, which are aligned with ISO 27001 and ISO 27002 requirements. The encryption ensures that sensitive data, whether stored in our primary systems or in backup solutions, is protected from unauthorised access.	
9.3	Encryption and Key Management	How are encryption keys managed?	Evidence of best practice key management policies and process.	Our PKI environment is managed and stored securely	
10.1	Governance and risk management	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? (e.g. tools for configuration management that can detect deviation from	We would expect some capability to detect accidental or deliberate configuration drift, either automatically or by frequent audit.	Yes, CNWL has the capability to continuously monitor and report compliance of our infrastructure against established information security baselines. We utilise advanced configuration management tools that can detect deviations from agreed configuration standards, allowing us to promptly address any discrepancies. Additionally, our systems are regularly audited to ensure adherence to security protocols, and compliance is reported to the Information Governance Board for oversight and action as necessary.	

10.2	Governance and risk management	Do you have agreements to ensure your providers adhere to your information security and privacy policies?	We would expect that any policies or procedures you apply to yourself are also applied to a similar or higher standard across your supply chain.	CNWL has established Information Sharing Agreements (ISAs) with all relevant providers to ensure adherence to our information security and privacy policies. These agreements are developed, reviewed, and signed off by key governance personnel, including the Caldicott Guardian, Data Protection Officer, and Senior Information Risk Owner. Additionally, we monitor compliance through regular performance meetings, ensuring that all subcontractors and service providers align with our information security management systems.	
10.3	Governance and risk management	Do you perform, at minimum, annual reviews to your privacy and security policies and controls?	We would expect periodic review of your privacy and security policies and controls to ensure they remain in line with industry best practice and are being carried out effectively.	CNWL conducts annual reviews of its privacy and security policies and controls. These reviews are integral to maintaining compliance with information governance regulations and ensuring that the policies are effective and up to date. The Information Governance Board oversees this process, monitoring compliance and making necessary adjustments based on the latest legislative requirements, audit findings, and evolving best practices in information security.	
10.4	Governance and risk management	How will you notify us if you make material changes to your information security and/or privacy policies?	We would expect to be notified of any significant changes to any of the information supplied in this assessment or the DPIA that may impact the security, reliability or availability of the service.	We will notify you through formal communication channels. This may include direct notifications via email, or through our regular contract and review meetings.	
10.5	Governance and risk management	Do you have a documented, organization-wide program in place to manage risk, with regular risk reviews?	We would expect some form of proactive risk management approach with risks periodically reviewed. This may be covered under a security methodology such as ISO27001 that you have adopted.	CNWL has a documented, organisation-wide program in place to manage risk, which includes regular risk reviews. This program is governed by our Information Governance Board (IGB), which oversees compliance with risk management processes and monitors key performance indicators (KPIs). Additionally, our risk management framework is aligned with ISO 27001 standards, ensuring that we adopt best practices for information security management. The central Information Governance Team (IGT) conducts ongoing risk assessments, updates the risk register, and ensures that all identified risks are managed effectively. This structured approach allows us to proactively address risks and implement necessary controls across our organisation to safeguard data and maintain compliance with relevant regulations.	
10.6	Governance and risk management	What cybersecurity accreditations do you have? ISO27001, Cyber Essentials + or other)	Please provide certificates along with SoA where applicable.	All NHS Trust have to meet the DSPT (Data Security and Protection Toolkit) standards set by the National Cyber and has an equivalence to Cyber Essential Plus	
11.1	Human Resources	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties that have access to Camden's data subject to background verification?	We would expect all employees that have access to Camden sensitive data to have been through some form of vetting.	Yes, all employment candidates, contractors, and involved third parties are subject to background verification checks. This process is outlined in our comprehensive information security policies and is monitored for compliance.	
11.2	Human Resources	Do you conduct Security awareness training for your employees?	We expect this to be an ongoing process and reviewed at regular intervals to ensure that it remains current & relevant.	Yes, all employees are required to undertake mandatory IG training	
11.3	Human Resources	Can you prevent access to sensitive Camden data by your employees or third parties contracted by you from BYOD, mobile and unmanaged devices, except when explicitly approved by Camden?	Camden data should be accessed from managed devices only.	There are no unmanaged devices accessing our systems. All devices used for accessing our systems are linked to employees, ensuring that only authorized personnel can access sensitive information. Furthermore, third parties do not have access to our systems, reinforcing our commitment to data security and compliance with information governance policies.	
12.1	Identity and Access Management	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	This is required	Yes, access to our systems is tightly controlled to ensure that only authorised personnel can interact with them. Comprehensive logging allows us to track and audit access events, enhancing our ability to detect any unauthorised attempts to access sensitive systems. Continuous monitoring further ensures that any anomalies or security incidents are identified and addressed promptly, maintaining the integrity and security of our information infrastructure.	
12.2	Identity and Access Management	What detection controls are in place to mitigate impact of unauthorized or inappropriate access?	Camden expects a level of control, to detect, prevent and or quickly recover from the impact of inappropriate access.	Access Logging and Monitoring: All access to information security management systems, such as hypervisors, firewalls, and APIs, is restricted, logged, and actively monitored. This enables real-time visibility of who is accessing the systems and what actions they are performing. Automated Alerts: The system is designed to trigger automated alerts in case of any suspicious or unauthorized access attempts. This allows for immediate investigation and response to potential security breaches. Regular Audits: Periodic audits of access logs are conducted to identify any anomalies or unauthorized access patterns. This proactive approach helps in detecting potential security incidents before they escalate.	
12.3	Identity and Access Management	Do you support the use of, Single Sign On (SSO) solutions to your service using Entra/Azure AD?	SSO is Camden's standard approach for authentication and is normally required for all production systems. Other access mechanisms need to be agreed on a case-by-case basis but would be expected to include multi-factor authentication and possibly other conditional access policies for high privilege accounts, alongside robust password management policies.	Yes, CNWL support SSO	
12.4	Identity and Access Management	Do user sessions time out after a period of inactivity?	Timeouts should be enforced to prevent sessions left hanging and then being used by unauthorised users.	Yes	
12.5	Identity and Access Management	Can the system prevent the use of concurrent logins for the same user id?	This should be prevented. Multiple sessions from the same login ID could indicate either a security breach or account sharing, with multiple users using the same login, which impacts auditability.	Yes the system does not allow concurrent access using the same login. If another tab is opened where the system is launched the previous tab which is logged in will logged out straight away. The system does not allow users to be logged in using multiple tabs or different login details at one go.	
12.6	Identity and Access Management	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	This is required	CNWL has implemented robust controls to ensure the timely removal of system access that is no longer required for business purposes. This includes role-based access control (RBAC), regular access reviews, and automated workflows for onboarding and offboarding employees.	
12.7	Identity and Access Management	How do you monitor and log privileged access (e.g., administrator level)	We expect access of privileged accounts to be monitored, logged reviewed on a regular basis.	Admin access is via MFA. The helpdesk has configured various permission groups based on job roles, such as Clinical, Administrator, and Read-Only. For example, a Consultant will be granted Clinical access, allowing them to perform clinical tasks, whereas an Administrator will not have permissions to prescribe medications. Any new permission requests or changes to existing permissions on a staff account are managed by the helpdesk. A ticket is logged for each request to ensure proper documentation and tracking.	
12.8	Identity and Access Management	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege, especially for admin accounts?	We would expect that highly privileged accounts are only used when necessary, from secured devices and from agreed locations (which can include home working provided suitable policies are in place). Ideally some form of Just In Time	Yes, this includes role-based access controls (RBAC) that limit permissions to only what is necessary for each user's role, particularly for admin accounts. Regular access reviews are conducted to ensure compliance, and access rights are promptly revoked when no longer required, minimising the risk of unauthorised access.	

12.9	Identity and Access Management	Does the application have integration with other services? If so what are the other options for secure authentication?	Camden is moving away from VPNs and has multiple cloud providers so cloud to cloud integration may be required, so some form of securely authenticated API based access (potentially exposed via the internet) is preferred for all interfaces.	System is not provided to Camden so no interfaces or connection to Camden cloud infrastructure	
12.10	Identity and Access Management	Describe the procedures and technical measures in place for data access and segregation of council data from other clients?	We are in favour of multi-tenanted architectures, but want to see evidence of appropriate logical separation measures. (Provide an architectural diagram of the application)	System is not provided to Camden so no interfaces or connection to Camden cloud infrastructure	
12.11	Identity and Access Management	Do you maintain a record of all personnel who have access to your IT infrastructure, including their level of access?	This is required	Yes, CNWL maintains a comprehensive record of all personnel who have access to its IT infrastructure, including detailed documentation of their levels of access. This record is regularly updated to reflect any changes in personnel, roles, or access permissions.	
12.12	Identity and Access Management	What controls are in place to prevent unauthorized access to your application, program, or object source code?	This is required	Yes, CNWL maintains a comprehensive record of all personnel who have access to its IT infrastructure, including detailed documentation of their levels of access. This record is regularly updated to reflect any changes in personnel, roles, or access permissions.	
13.1	Infrastructure security	Are there any host-based and/or network based IDS/IPS intrusion detection/prevention mechanisms to detect and facilitate the analysis and investigation of incidents?	Host based and network based IDS and A/V tools are normally expected. The controls will differ depending on the solution and what is already provided by the hosting provider.	IDS / IPS services are implemented across the network infrastructure	
13.2	Infrastructure security	Are there standard APIs used to access the service, and if so can you provide Camden with a list of them and how they should be used?	Where there is a possibility that programmatic access to the system via APIs would be useful from other systems (for instance for automation purposes), we would expect APIs to be available with sufficient coverage to perform all the operations Camden is likely to need.	No APi's into Camden network / connectivity	
13.3	Infrastructure security	Does the application maintain activity logs of: 1. Authentication attempts 2. configuration changes 3. File /user activity 4.Are logs Centrally stored and retained for how long?	We would expect processes to manage logs and retain for suitable periods in a tamper proof manner. We would expect logs to be maintained for at least 30d as a minimum.	Log records are maintain of all user access	
13.4	Infrastructure security	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)? & Can the logs be made to Camden in a suitable format when required?	We would expect evidence (such as a policy document stating frequency and how) and that logs are reviewed for alerts and suspicous activity.	Logs are reviewed as required	
13.5	Infrastructure security	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Required, in order to ensure accurate traceability of events across logs from different systems.	Domain members servers, source NTP is domain controllers.	
13.6	Infrastructure security	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	This is required.	Yes - These are monitored	
13.7	Infrastructure security	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	This is required.	Yes	
13.8	Infrastructure security	How do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails)?	We would expect access to the hypervisor or equivalent layers to be very tightly controlled.	All access to hypervisors is strictly controlled by Rackspace who manage the infrastructure, non-approved staff cannot access the infrastructure.	
13.9	Infrastructure security	Are there any other technical measures or defence-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-		Packet level inspection is undertaken	
13.1	Infrastructure security	How do you deal with Zero-day vulnerabilities?	We would like to understand your strategy and keeping the Council informed.	Zero day NHS CareCert are issued and remediated within 14 days	

13.11	Infrastructure security	Will your application work behind a Web application firewall (WAF) to protect it from OWASP top 10 attacks such as XSS, SQL injection and others?	We are expecting an added layer of protection from these types of attacks.	Yes, our application is designed to work seamlessly behind a Web Application Firewall (WAF). The WAF provides an additional layer of security by filtering and monitoring HTTP traffic between the application and the internet.	
14.1	Security Incident Management	Do you have a documented security incident response plan that is periodically tested at least annually?	This is expected.	Yes	
14.2	Security Incident Management	Are you registered with the ICO? Have you notified the ICO of any data protection incidents within the last 12 months? (***If your is yes please provide details***)	Report data breach to ICO within 72 hours and Camden Council must be notified within 24hrs. We would expect to see the details of the incident, the incident remediation plan, recovery timeline.	Central and North West London NHS Foundation Trust (CNWL) is registered with the Information Commissioner's Office (ICO). There have been no reported incidents in the last 12 months by Sexual Health and HIV Services. All incidents are reported through the Trust adverse incident management system and guarded using the NHSE data protection breach assessment matrix.	
14.3	Security Incident Management	How do you monitor and quantify the types, volumes, and impacts of all information security incidents?	We would expect you to have a good understanding of the security incidents that have affected you.	The National SoC identifies incidents which we would then resolve locally, there have been no Incidents impacting services in last 12 months. All Data protection and security incidents are categorised and reported on a monthly basis to the Trust IG Board where lessons learned and additional technical measures required are discussed and recorded	
15.1	Supply Chain Management	How are your controls designed and implemented to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	Where there is 3rd party dependency we expect thorough risk assessment policies or contractual agreements in place.	Security requirements and certification are included within our specifications and Contractual Terms for all suppliers	
15.2	Supply Chain Management	Where you are prime supplier, what responsibility do you take for any security incidents with the services and products supplied to us that may be caused by your 3rd party suppliers or contractors?	We would expect some form of contractual responsibility for your supply chain in your contract with us.	We take full responsibility for any security incidents related to the services and products we provide, including those caused by our third-party suppliers or contractors. We ensure that all third-party suppliers and contractors adhere to our stringent security standards and protocols. In the event of a security incident, we will promptly address the issue, mitigate any potential damage, and implement corrective measures to prevent future occurrences.	
16.1	Accessibility	Does the product or service conform to any relevant accessibility guidelines such as the Web Content Accessibility Guidelines Web Content Accessibility Guidelines (WCAG) 2.1 (w3.org). Services must achieve WCAG 2.1 level AA as part of meeting government accessibility requirements.	This is a legal requirement.	Yes	
17.1	Data Standards	Can you make the data model for the system available to Camden so we can understand the data being held and check it aligns with Camden data standards, master data management, and reporting needs	We want to ensure that, should we ask for this, you can make it available.	While we are unable to provide the data model directly, we are more than happy to liaise with Camden to ensure that you have a comprehensive understanding of the data being held. We can work together to verify that it aligns with Camden's data standards, master data management, and reporting needs. Our commitment to transparency and collaboration remains strong, and we are dedicated to supporting your data governance objectives	
17.2	Data Standards	Is there a way of identifying all data that has changed since a particular point in time, should Camden need to extract data that has changed to update other systems that also use this data.	This would typically be done via a "last updated" column in database tables, which can be queried against over ODBC.	Whilst it is easy to identify when a record was last updated, we are not able to provide access to our database as it contains confidential medical records	
18.1	Non live environments	How do you maintain consistency between non live and live environments - so that changes made to one environment can be easily applied to another	For instance, we would expect it to be easy to create new test environments that are based on the current live configuration (but with dummy data).	We test code updates on our test environment prior to uploading to the production service. The system has a live environment and a test environment. These are maintained in line with each other in terms of functionality. The test environment has test data and dummy patients.	