FAO; IT Security Officer
Information Management & Technology
Mailpoint 79
Southampton General Hospital
Tremona Road
Southampton SO16 6YD
Tel: 023 8120 5713

System Level Security Policy (SLSP)

February 2020 Revision

Introduction:

The development, implementation and management of a System Level Security Policy (SLSP) will help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

An effective SLSP will therefore contain a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.

In the context of this document "System" relates to the complete data handling solution (electronic or otherwise) of patient identifiable / sensitive data.

Current encryption guidance for NHS organisations can be found at https://www.igt.connectingforhealth.nhs.uk/whatsnew.aspx?tk=401326148792982&cb=14%3a46%3a41&lnv=2&clnav=YES (Select: "Encryption Guidance 31.1.2008.doc"), and we would expect any electronic solution for the handling of patient identifiable / sensitive data to comply with this guidance as a minimum.

Where the system is available to multiple organisations, the SLSP must establish the necessary common policy, security parameters and operational framework for that system's expected operation including any functional limitations or data constraints applicable to one or more bodies.

The SLSP is a core component of an accreditation documentation set for those organisations that undertake formal accreditation processes for their information assets.

This document has amended from its original created by the National Information Governance Board (NIGB) for Southampton University Hospital Trust (UHS).

The following series of topics are relevant for any system level security policy and are intended to help guide responsible staff through their considerations for the development of their system level security documentation. This list is not exclusive of all possibilities and it is the responsibility of each organisation to identify and consider their security management needs on a case by case basis. This is best achieved through a formal process of risk assessment and mitigation.

SUHT System Level Security Policy
(SLSP)

System Details	
1. The System shall be known as:	• My Medical Record
2. The System's responsible owner shall be: *(Please state the post/job title)*	• Kevin Hamer, My Medical Record Programme Manager
3. The System's Caldicott Guardian shall be:	• Gail Byrne, Director of Nursing, UHS.
System Security	
4. Security of the system shall be governed by: *(Please choose; Trust Policy, External Organisation Policy or Local System Manager and state policy name; and person(s) responsible)*	• Data Protection Act • Caldicott guidelines • Microsoft Azure security
5. The System's responsible security manager shall be: *(Operational manager or equivalent. Please state the post/job title)*	• Paul Gisborne, My Medical Record Technical Delivery Manager
6. The security manager duties shall include: *(For example: Initial security sign-off of the system, accreditation, annual reporting/inspection of the system security)*	• Agree system design • Management of change control and testing of all system changes inc. software upgrades • Co-ordination of penetration testing and applying recommended security measures
7. The System shall incorporate the following security countermeasures: *(Where applicable, please explain further)*	
Physical Security Measures:	
✓ Storage location of System *(Hardware)*	• Microsoft Azure cloud hosted service
Logical Security Measures:	
✓ Users have signed Information Sharing agreements	• N/A but all users are covered by data protection sign up.
✓ User Access control/Privilege Management	• Clinical access is restricted to individual user as required
Network Security Measures:	
✓ Encryption level of System and data in electronic transit *(AES 128/256, SSL, DES)*	• All connections to and from web server, data store and TIE are SSL
✓ Networked Hardware or Standalone system	• Networked – web and data store are physically

	and logically separate (in same Azure instance)
✓ Antivirus	• Antivirus is built into cloud hosted platform
✓ Firewall	• There is a firewall controlled secure connection between the Azure cloud and internal network data stores
Other:	
✓ Scheduled system review	• Regular penetration tests, co-ordinated by Networking team • DPIA has been completed (this will be reviewed yearly at a minimum)
✓ Other Authentication or Certification Arrangements	• Just SSL cert
✓ Back Up Arrangements	• As per Microsoft Azure policies
Additional Notes: *(Please add any details not included in the sections above)* *Technical, operational and procedural countermeasures should include reference to standards used where these are known NHS organisations are required to comply with the range of best security management practices as set out in the BS7799 / ISO 27002.*	

System Management

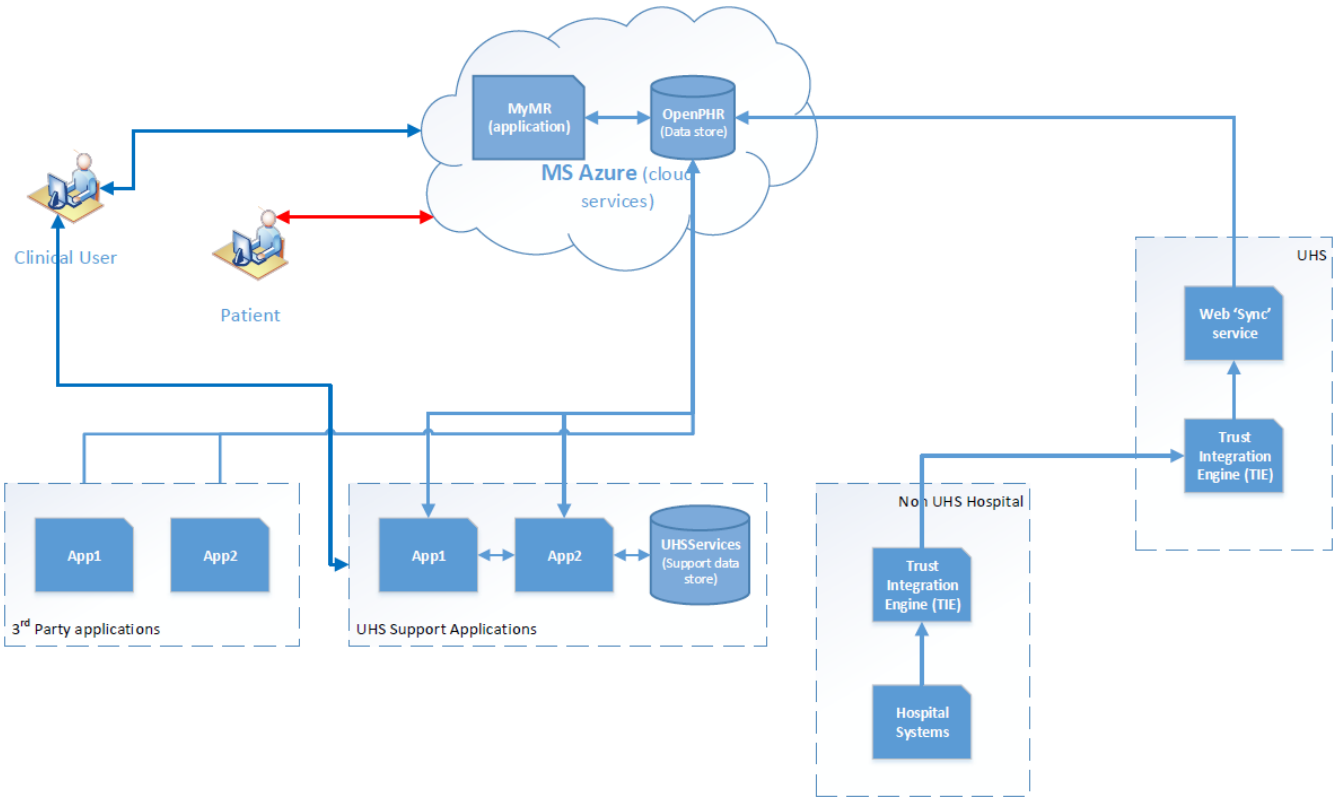
8. The System has been developed by: *(Supplied System/In-House Development)*	• Get Real Health (supplier) • Software solution augmented with additional code developed internally
9a. The System shall be implemented by:	• My medical record team (supported by supplier)
9b. The System shall be maintained by:	• My medical record team (supported by supplier)
9c. If this is an externally supported system does the Service Level Agreement (SLA) include references to Incident Reporting procedures and response to Incidents?	• Yes
9d. Are there formalised plans for conceptualisation, development,	Service already live. We have a standard

implementation, testing, acceptance, maintenance and end of life for the system. *(Not all stages will be applicable, however end of life/disposal of the system should be discussed in Q16)*	process for upgrades etc. based on the way the supplier software works.

10. Will the System be shared or used by any other organisations. Please identify this relationship, along with Contractual obligations and Information Sharing Agreements between the parties.	• Other hospitals use the service and we have a mix of documentation dependent on the requirements of that hospital (typically their IG team). So, we have a mix of DPIA, SLA, Information Sharing Agreement, IG compliance documents but this is different for each site.

System Design

11a. The System shall comprise:
(Please describe the systems design, this should show the device(s) (E.g. file server) where the data will reside, links to any wider network clouds (E.g. site LAN, Internet and / or any other external networks), and any relevant firewalls / gateway control devices. (E.g. below)



Example: *"The database will be held on an encrypted hard drive using TrueCrypt software with AES encryption. The hard drive will be in a single desktop computer which is not networked. The computer is kept in a locked office, is accessed only by XXXXXXXXXX and XXXXXXXXXX under his direct supervision and the office is on a locked corridor at SUHT. The database will be backed up onto an encrypted external hard drive in a locked filing cabinet in the same locked office".*

11b. Describe the means by which unauthorised access to the system and its data will be prevented.	• Handled by login/password to the supplier software, this has been penetration tested • Data is kept separate and secure from the web server

Operational & Data Processes

12. Please state where patient identifiable/sensitive data will be collected from at points within the system: *(Security arrangements per input/out need to be identified. Remember, local IT and IG Policies which are mandated on the Trust. These address technical areas such as, security access control, firewalls, antivirus, updates, data loss prevention and so forth)*	• The entire system is designed to collect, store, update patient information but this is done either by the patient or at their consent (through UHS feeds). There is a rigid consent process on first sign up.

13. The data will be stored and subject to :	
• In what format (paper/electronic)	• Electronic
• If the Data contains PID, please describe the anonymisation process.	• Only 1 record can be accessed at a time, either by the patient themselves or the clinical team to whom they have given access • All reporting/export is anonymous (no patient identifiable data is included, just a number that is not linked to PID or other unique IDs)
• Will back-up's be encrypted; to what standard.	• As per server policy

14. The data will be processed:	
• List the device types the system will be accessible on. E.g. PDA's, Laptops, PC's, COW's.	• Any internet enabled device
• State whether these devices cache or store data, if so indicate encryption to be employed.	• No data can be stored or cached
• State whether remote access (over the Internet or otherwise) will be employed to access the data	• All access is over the internet (even for internal staff) since the service sits in the DMZ outside of

	UHS network
• Describe measures in place to prevent the interception of transmitted data (E.g. standalone network, encrypted path, SSL (https) website etc)	• All communication between end user, web server, and UHS network (data store and TIE) is secured by SSL

15. The System's authorised users shall be: *(All parties should have signed the necessary agreements to ensure details from the IT Security, Data Protection and Information Sharing policies are upheld.)*	• All registered patients (signed up at their consent) • Designated clinical team members (as determined by clinical lead). All existing UHS users bound by DP/Caldicott
15a. Where a Super User has been identified to manage a system, are:	
✓ **Super Users appropriately approved by their superiors?**	• N/A
✓ **Are Super User actions routinely approved/audited?**	• N/A
✓ **Do Super Users raise system and access breaches to management teams and IM&T when required?**	• N/A
16. When the system or its data has completed its purpose/has become redundant or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data: *(Please identify any data retention period and method of data destructions once this has passed)*	• There is no data retention period. Data stored in the patient record is managed by the patient.
17a. Who should Users of the system report Information Security Events (Incidents) to? *(Eg. Supervisor, System Manager, IM&T Helpdesk)*	My medical record team (mymedicalrecord@uhs.nhs.uk). Incidents are then handled by MyMR Programme Manager and Trust Records Manager. Patients report in this way too.
17b. Has this been communicated to all users as part of their system training?	• Yes
<u>System Audit</u>	
18. The System shall benefit from the following internal/external audit arrangements: *(Annual audit, Internal or External)*	• Regular internal PIA which is assessed externally • Process completed once a year at a minimum

19. Please state how often the system will be risk assessed.	• As above

System Protection

20. The System shall benefit from the following resilience/contingency/disaster recovery arrangements:	• As per server policies • Hosted in Microsoft Azure

Example: *"Back up onto encrypted external hard drive in a locked filing cabinet, stored in a locked office in a locked corridor. There will also be 5 year data retention for audit purposes; this will also act as a disaster recovery restoration plan."*

21. In the event of serious disruption or total system failure, business continuity shall be provided by the following means:	• Restore as per server policies. • N.B. Not strictly needed as part of business continuity due to the nature of the service

22. In the event of a security or confidentiality breach occurring the following procedure shall be followed:	• All events/incidents are reported to the Trust Records Manager who will follow standard Trust reporting procedures based on Information commissioner guidelines.

SUHT's IT Security and Data Protection Officers should be contacted, who will then implement investigations as per Trust Procedure. More information on this is available in the IT Security and Data Protection Policies. (Available on StaffNet).

System Level Security Policy Ownership

23. **This SLSP shall be the responsibility of** *(The System Manager or Other)*	• Kevin Hamer, My Medical Record Programme Manager

24. Please state if this SLSP will be distributed as part of any documentation or application process. *The SLSP will be held by the System/Asset Manager and IM&T, and will be subject to FOI requests.*	Data in the system is not subject of FOI/SAR requests. The service provides a patient record (one they own) but is different from (and does not represent) the hospital record.

Data Protection Registration

25. Please confirm that your organisation has Data Protection Registration to cover the purposes of analysis and for the classes of data requested. *(Available from the Data Protection Office)*	The Data Protection Registration (ICO) Number of UHSFT is: Z4989884 Expiry Date: 27/11/2020 Registration document available on request.