# PharmOutcomes System Assessment Template

The following template has been provided with pre-populated information to assist Information Asset Owners in hospital trusts document their use of the PharmOutcomes systems   
May 2018

|  |  |  |
| --- | --- | --- |
| 1. | Governance and Roles |  |
| 1.1 | System Name | PharmOutcomes and Outcomes4Health |
| 1.2 | IAO and Job Title |  |
| 1.3 | IAA and Job Title |  |
| 1.4 | Caldicott Guardian | Pamela Bowes |
| 1.6 | SIRO | Gary Warner |
| 1.6 | Next Review Date |  |

|  |  |  |
| --- | --- | --- |
| 2. | Purpose of the System |  |
| 2.1 | Simple overview of the purpose of the system | PharmOutcomes/Outcomes4Health (the system) is a secure, web-based clinical and service management data collection and communications platform that allows patient-facing entry of service information and personal sensitive data. Encryption levels and system design make The System suitable for recording and storing patient-sensitive data and meets the requirements of Data Protection Regulations, including GDPR, and Level 3 of the NHS Information Governance Framework.  The system is used by [Your Organisation] to support the provision of services by [community pharmacies/general practitioners/third-sector providers]. |
| 2.2 | Scope/ access | *Within the commissioning organisation* The system has approximately [X] users  *Within provider organisations* The system will be used by approximately [X] provider organisations  *Reporting of Information* Anonymised data from the system is used to report activity to [X] |

|  |  |  |
| --- | --- | --- |
| 3. | Software |  |
| 3.1 | Details of software where applicable | *PharmOutcomes is a secure internet-based system. It will run on any currently supported full featured browser with javascript enabled. No information or service is stored on commissioner’s servers or user’s computers, beyond those items that they manually download and cached images, except a single browser cookie which maintains state between transactions and is strictly necessary for system operation.*  The system is designed, developed and maintained by: Pinnacle Health Partnership LLP Registered Address: 1st Floor Weatherwise Building, Well Road, East Cowes PO32 6SP  A license for [multiple services/a single service] are held for [X] providers |

|  |  |  |
| --- | --- | --- |
| 4. | Hardware |  |
| 4.1 | Details of hardware | PharmOutcomes/Outcomes4Health is held on a secure server infrastructure hosted entirely within the UK by Memset Ltd, Building 87, Dunsfold Park, Stovolds Hill, Cranleigh, GU6 8TB and Unit 2, Smallmead Road, Reading, RG2 0QS.  The Data Centre is accredited to HSE standard to house the PSN - (Public Services Network) Assured and PSN Protected networks  Memset operates an ISO 27001 certified Information Security Management System that provides mature, scalable and audited management of security policy, issues and continual improvement. |

|  |  |  |
| --- | --- | --- |
| 5. | Data Retention |  |
| 5.1 | Details of the data collected and recorded on the system | The records entered onto PharmOutcomes by providers remain their data as Data Controllers and forms part of a clinical record for a healthcare professional/provider.  This information is held by PharmOutcomes/Outcomes4Health for as long as necessary. Please consult the current NHS guidelines <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>)  In the event that the service is terminated prior to the end of that period, providers are able to download and/or print a copy of their records in order to retain them for the appropriate period of time.  The information asset owner for the Commissioner is responsible for ensuring that data is retained for the appropriate retention period and then deleted. |

|  |  |  |
| --- | --- | --- |
| 6. | Physical Security |  |
| 6.1 | Physical Security details | Having two data centres allows us to maintain a live copy of all data in two physical locations providing us increased resilience over a single data centre. The two data centres are connected by a dedicated fibre line separate from the main internet.  • 8,500 Solar panels on-site  • Diverse power feeds to substation  • N+1 Generators with at least 36 hours of fuel on-site and refuel provision  • N+1 UPS with capacity for full data centre.  • N+25% Adiabatic Coolers for main data centre hall and Air Conditioning for UPS batteries.  • Biometric authentication system  • Data centre located inside its own secure compound  • Fencing and electric entry, including vehicle control systems  • FM200 Waterless Fire Suppression System  **Round the Clock Monitoring**  Every system within the data centre is monitored and controlled from the on-site control room and maintained 24 x 7 x 365.  **Physical Security**  Access to the data centre is strictly controlled, with manned security on-site 24/7. All access points in the data centre are monitored by dedicated internal security, utilizing individual card swipes, biometric scanners and CCTV. Security coverage spans from the heart of the facility to the outer compound.  **Uninterrupted Power Supply**  Should mains supply fail at any time, a series of generators seamlessly kick-in to power all hosted equipment supported by site-wide UPS system. Generators run for 36 hours with onsite fuel and are refuel-able in use.  **Cooling**  The adiabatic cooling system is configured with N+25% built-in redundancy for when the data centre is operating at maximum capacity. |

|  |  |  |
| --- | --- | --- |
| 7. | Access Control |  |
| 7.1 | Who is responsible for controlling access to the system | Individual providers are responsible for authorising individual users within their organisation.  The commissioning organisation is responsible for authorising individual users within their organisation. Their job roles are [X]. |
| 7.2 | Who gives approval and what record is kept | [X] is responsible for setting up new users and this is recorded in [X]. |
| 7.3 | Are users given unique id’s/ Is there a system admin role | All users are given their own unique login and password.  The commissioning organisation and the person noted at 7.2 above can provide differing levels of access, as required and appropriate.  There are no generic codes. |
| 7.4 | Password length requirement | The length of passwords will always be checked automatically at the time that users construct or select them. A User Password must contain a minimum of eight (8) characters. |
| 7.5 | Password changes | We are moving away from forcing password changes following the [guidance of the National Cyber Security Centre](https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry) which has determined that this makes systems less secure. This can be changed at the request of the commissioner to meet their own policy. |
| 7.6 | Inactivity log out | After 10 minutes users are required to confirm their intention to continue working. After a further 5 minutes they must enter letters from an additional security word beyond their password to unlock the system |
| 7.7 | Logon attempts | The number of unsuccessful consecutive logon attempts is restricted to 3 |
| 7.8 | Procedure for when access is no longer required | The Commissioner is responsible for removing users who no longer require access |

|  |  |  |
| --- | --- | --- |
| 8. | Access Rights |  |
| 8.1 | Details of access rights | Access rights are available to users with Admin/Users rights granted and can reset passwords for other users.  Individual restrictions can be set for Services, Claiming, Reporting and Admin at various levels.  Access rights will be reviewed on an annual basis by the Commissioner Information Asset Owner. |

|  |  |  |
| --- | --- | --- |
| 9. | User Training |  |
| 9.1 | Details of any specific training | Training is provided by Pinnacle Health Partnership free of charge twice a year at site throughout the country or can be commissioned at other intervals.  [X] is responsible for immediate new user training |

|  |  |  |
| --- | --- | --- |
| 10. | Risk Assessment |  |
| 10.1 | Details of risk assessment and next review date | A risk assessment will be undertaken following the Information Asset Management procedure. This will be performed on an annual/ quarterly basis. |

|  |  |  |
| --- | --- | --- |
| 11. | Data Protection/Caldicott |  |
| 11.1 | Subject access requests/ functionality to respect objections/withdrawal of consent | Subject access requests can be met within one month in accordance with GDPR requirements |
| 11.2 | Any specific requirements regarding consent and disclosures of information | Initial requests for SARs should be directed to iow.pinnacle@nhs.net from a secure nhs.net address |

|  |  |  |
| --- | --- | --- |
| 12. | Relevant Legislation/ Contractual Obligations | . |
| 12.1 | Details of any specific legislation e.g. Mental Capacity Act 2005, Children Act 2004 | No relevant legislation applies |

|  |  |  |
| --- | --- | --- |
| 13. | Audit Trails |  |
| 13.1 | Details of any audit trails provided | The system maintains user and organisation level activity within an audit of service activity which is provided on screen and csv formats.  Detailed audit trails are maintained for all clinical service data transactions which can be interrogated upon request and granting of appropriate permissions. |

|  |  |  |
| --- | --- | --- |
| 14. | Data Quality |  |
| 14.1 | Details of any data quality requirements | The system allows commissioners to restrict data entry to meet set requirements or be within criteria defined by the commissioner. Records cannot be saved until the requirements are met. |

|  |  |  |
| --- | --- | --- |
| 15. | Data Backup | |
| 15.1 | Details of any data backup arrangements | The primary systems are replicated live to secondary systems. The system is also backed up live to another data centre every four hours on an incremental basis and a full system backup taken each evening. |

|  |  |  |
| --- | --- | --- |
| 16. | Auditing Compliance |  |
| 16.1 | Details of who is responsible for auditing compliance. e.g. confidentiality audits | Audits are undertaken by [X] on a [monthly/quarterly/annual] basis. |

|  |  |  |
| --- | --- | --- |
| 17. | Security Incident Management and Reporting |  |
| 17.1 | Details of how to report an incident | All suspected or actual breaches of security regarding the system are to be reported to the Information Asset Owner who will report via NHS England’s incident reporting procedure if appropriate |

|  |  |  |
| --- | --- | --- |
| 18. | Business Continuity |  |
| 18.1 | Details of any business continuity plans | When data is entered onto PharmOutcomes, there is no information stored locally on the pharmacy computer, so fires, burglaries and computer failure at the provider will have no impact.  The PharmOutcomes systems are located in ISO27001:2013 accredited data centres in England operated by Memset Limited, our hosting partner and all the operational staff who have access to the system are security vetted.  The disaster recovery and business continuity arrangements for PharmOutcomes are part of the core design of the system. Failover protection is provided by dual load-balancing servers and dual web-servers. As soon as records are saved by a contractor on the PharmOutcomes platform, e.g. by clicking a 'Save' button, a record is made on the PharmOutcomes database system which is located in England, and an identical copy is replicated onto another two servers in two distinct data centres.  The system is run across two data centres with data always stored on both sites. In the event that a whole data centre was lost the system would failover all primary users to the second automatically within a few minutes. A full system backup is taken each evening.  Pinnacle Health Partnership also maintains backup support premises with full facilities which ensures that support can be continued if the primary location is compromised.  All of our business continuity arrangements are accredited by ISO27001 and are subjected to a complete crash test check every year (or whenever infrastructure changes make reverification appropriate). |