PharmOutcomes
Delivering Evidence

PharmOutcomes Information Governance

and

Technical Specification

PharmOutcomes®

Information Governance

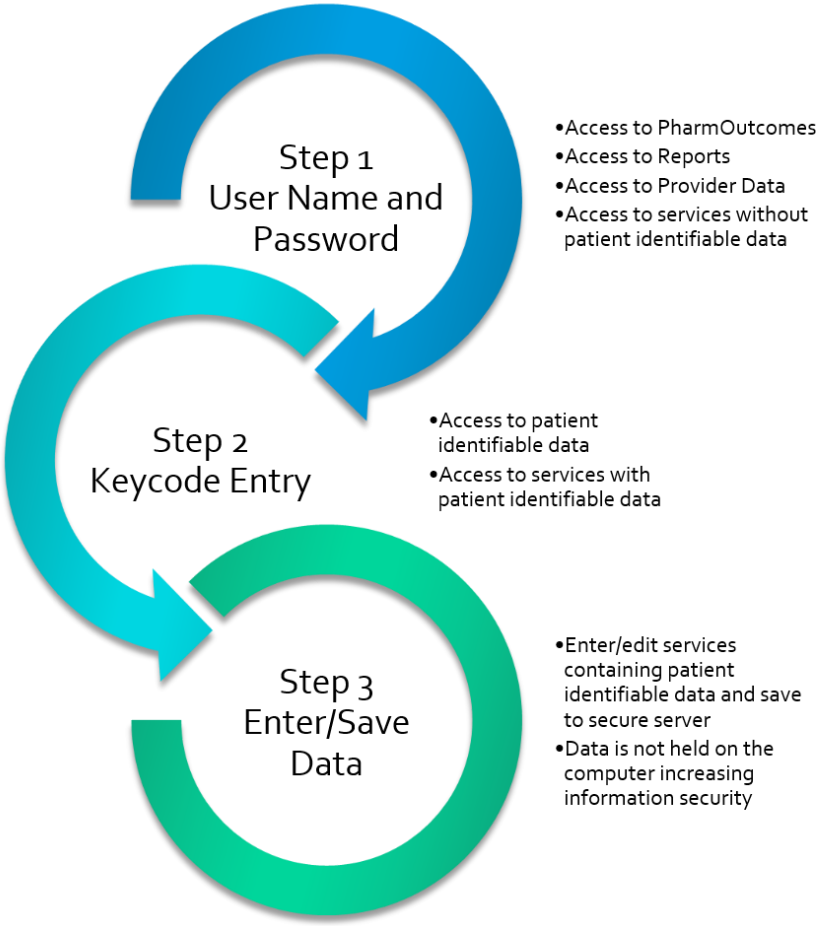
As patient identifiable data is stored on PharmOutcomes it is imperative that information governance requirements are fully met. PharmOutcomes has been designed to be compliant with the Data Protection Act. The data controllers and processors of the data is described and explained in the PharmOutcomes Data Ownership Guidance. No patient identifiable information will be accessed or used by anyone other than the appropriate data owner or authorised and monitored system support staff undertaking system maintenance.

PharmOutcome redacts patient identifiable information and provider information at the different levels to ensure that confidentiality is maintained

The PharmOutcomes User Agreement details the relationship between PDS Ltd and the pharmacy contractor. PDS Ltd took expert legal advice to allow it to review its procedures and to develop the PharmOutcomes User Agreement that sets out the respective obligations of pharmacies, of PDS and of the sub-contractors used by PDS Ltd. All pharmacies and their staff accessing PharmOutcomes have to accept the terms of the PharmOutcomes User Agreement.

The PharmOutcomes Service Level Agreement details the relationship between Pinnacle Health Partnership LLP and the system commissioner.

Each pharmacy contractor can setup and delete user logons for their own pharmacy in order to give appropriate access to their staff. There is a triple level secure log on requiring their user name, password and a 6 character security word.



For security and audit purposes, the system retains a full log of all user activity; the logs are auditable given an appropriately authorised and legal request to do so.

PharmOutcomes' information security policy, security management and practices have been specifically designed to be meet with the Level 3 requirements published by the NHS for 3rd party commercial providers and to be compliant with the NHS code on confidentiality. PDS Ltd ensures that it, and the company that hosts the PharmOutcomes platform and the company that processes the data are compliant with the Data Protection Act, and have industry level standards of protection.

Pinnacle Health has commissioned independent testing of the PharmOutcomes platform to ensure that there can be no unauthorised external penetration and also an independent test of vulnerability internally (i.e. the threat of misuse by an authorised user) and these have confirmed that PharmOutcomes has robust security in place.

PharmOutcomes is designed to use the maximum level of encryption supported by the user's browser application. Typically the connections are encrypted via a secure 256 bit encrypted link where the user's browsers are capable and, in any event, to refuse a connection for anything less than 128 bit AES.

PharmOutcomes®

IG Toolkit Assessment Summary Report

Pinnacle Health Partnership
(NHS Business Partner/ITC/ALB)
Prepared on 31/03/2016

Information Governance Management

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Not Relevant	Total Req'ts	Overall Score	Self-assessed Grade	Reviewed Grade	Reason for Change of Grade
Version 13 (2015-2016)	Published	0	0	0	5	0	5	100%	Satisfactory	n/a	n/a

Confidentiality and Data Protection Assurance

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Not Relevant	Total Req'ts	Overall Score	Self-assessed Grade	Reviewed Grade	Reason for Change of Grade
Version 13 (2015-2016)	Published	0	0	0	8	0	8	100%	Satisfactory	n/a	n/a

Information Security Assurance

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Not Relevant	Total Req'ts	Overall Score	Self-assessed Grade	Reviewed Grade	Reason for Change of Grade
Version 13 (2015-2016)	Published	0	0	0	11	2	13	100%	Satisfactory	n/a	n/a

Clinical Information Assurance

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Not Relevant	Total Req'ts	Overall Score	Self-assessed Grade	Reviewed Grade	Reason for Change of Grade
Version 13 (2015-2016)	Published	0	0	0	3	0	3	100%	Satisfactory	n/a	n/a

Overall

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Not Relevant	Total Req'ts	Overall Score	Self-assessed Grade	Reviewed Grade	Reason for Change of Grade
Version 13 (2015-2016)	Published	0	0	0	27	2	29	100%	Satisfactory	n/a	n/a

Grade Key

Not Satisfactory	Not evidenced Attainment Level 2 or above on all requirements (Version 8 or after)
Satisfactory with Improvement Plan	Not evidenced Attainment Level 2 or above on all requirements but improvement actions provided (Version 8 or after)
Satisfactory	Evidenced Attainment Level 2 or above on all requirements (Version 8 or after)

Version 13 (2015-2016) History

Status	Date
Published	31/03/2016 11:10
Started	16/07/2015 10:16

Pinnacle HEALTH PARTNERSHIP

Data Protection Act and Data Ownership

In the PharmOutcomes system, providers enter data to a specification set by service commissioners; PharmOutcomes then acts as an anonymisation service to allow commissioners to see both aggregated service data and records concerning patients and clients without identifiable details. This is all done within the framework of the Data Protection Act 1998, which has eight principles that PharmOutcomes upholds:

- Personal data shall be processed fairly and lawfully;
- Personal data shall be obtained only for one or more specified and lawful purposes;
- Personal data shall be adequate, relevant and not excessive;
- Personal data shall be accurate and, where necessary, kept up to date;
- Personal data shall not be kept for longer than is necessary;
- Personal data shall be processed in accordance with the individual's rights;
- Information must be kept secure; and
- Personal data shall not be transferred to a country or territory outside the European Economic Area.

The Act further defines the activities of users or organisations, and in the case of PharmOutcomes these are:

- Providers – Data Controller and Data Processor
- PharmOutcomes – Data Processor
- Commissioner – Data Controller

This, together with the End User License Agreement helps define ownership of "data" in its various forms.

Providers

The records entered onto PharmOutcomes by providers remain their data because it can form part of a clinical record for a healthcare professional/provider. This information is held by PharmOutcomes for as long as necessary under the current NHS guidelines (Records Management NHS Code of Practice Part 2 (2nd Edition) Annex D1 indicate minimum retention periods and required final actions). Providers are able to download and print a copy of their records in order to retain them for the appropriate period of time. After that period providers will be contacted regarding the redaction, archiving or deletion of the information depending on existing NHS guidelines at that time.

Records should not ordinarily be kept for longer than 30 years. The Public Records Act does, however, provide for records, which are still in current use to be legally retained. Additionally, under separate legislation, records may be required to be retained for longer than 30 years (eg Control of Substances Hazardous to Health Regulations). The minimum retention periods should be calculated from the beginning of the year after the last date on the record. For example, a file in which the first entry is in February 2011 and the last in September 2014, and for which the retention period is seven years, should be kept in its entirety at least until the beginning of 2022. Each organisation should produce its own retention schedules in the light of its own internal requirements.

The records do not belong to Pinnacle Health Partnership LLP, the providers of PharmOutcomes. As a social enterprise, one of our aims is to evidence the value that community pharmacy brings to commissioners. The End User License Agreement (EULA) does allow us to use the Anonymised Information, and aggregate it, for use for purposes which Pinnacle and Health Information Exchange/PSNC reasonably consider to be of benefit to the interests of the pharmacy community as a whole to meet this aim.

Commissioners

The EULA and Service Level Agreement (SLA) with commissioners allows them broader rights to view and act with the data as they see fit. Obviously, this is within the confines of the eight principles of the Data Protection Act and the additional requirements of the Caldicott Guidelines, which were reviewed and updated in 2013. However, they do not have rights to restrict the activity of providers to manage their own data as they similarly see fit, other than as part of post-payment verification and validation.

Traditionally, some commissioners may have wanted to see identifiable information to "track" an individual through a care pathway. However access to this is not generally deemed appropriate, without explicit consent having been obtained from the patient/client. In an example regarding disclosure of patient data to NHS managers and the Department of Health (e.g. commissioning, prescribing advisors, financial audit, resource allocation etc.), *Confidentiality - NHS Code of Practice* states:

The use of anonymised data is preferable for management purposes but this is not always practicable. Systems that are capable of providing anonymised data sets for management purposes should be developed. Where they do not yet exist, the use of confidential information to support these activities may well be appropriate and necessary, but care should be taken to determine the minimum requirements.

Explicit consent is required unless there is (rarely) a robust public interest justification and, in the absence of either, support is required under section 60 of the Health & Social Care Act 2001.

PharmOutcomes has the ability to manage this process for commissioners, providing reports such as duration of care to remove the need to access identifiable client data, thereby protecting both clients and commissioners.

PharmOutcomes®

System Requirements

PharmOutcomes is an internet based system. It will run on any currently supported full featured browser with javascript enabled.

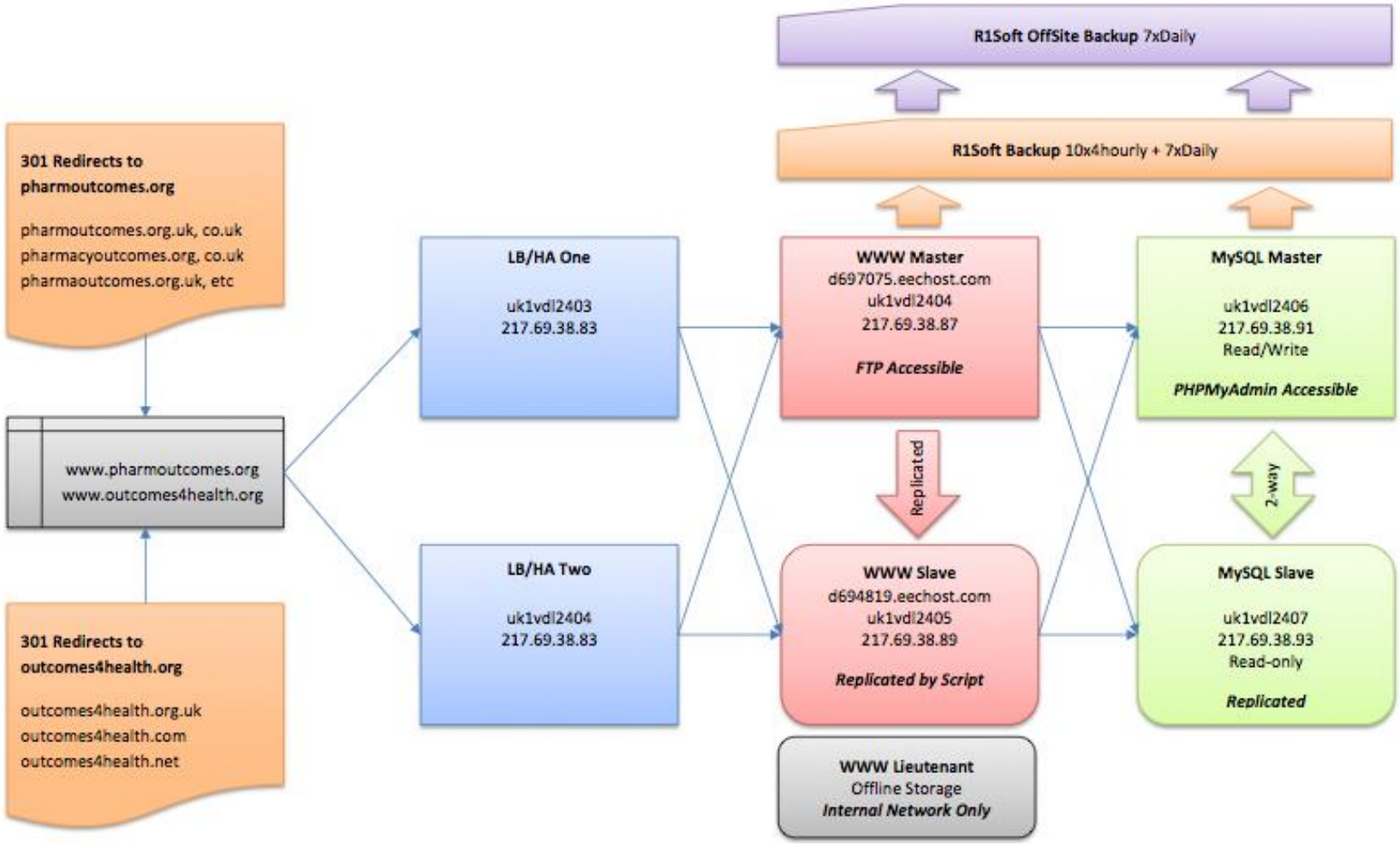
This includes:

- Internet Explorer 8 or greater
- Chrome
- Opera
- Firefox
- Safari

No information or service is stored on commissioner's servers or user's computers, beyond those items that they manually download and cached images, with the exception of a single browser cookie which maintains state between transactions and is classified within UK and EU cookie law as "strictly necessary. The formal cookie policy can be found through a link at the bottom of each page of the PharmOutcomes system.

PharmOutcomes®

Technical Solution Diagram



Pinnacle HEALTH PARTNERSHIP

Technical Infrastructure and Resilience

Network

What speed/capacity Internet links are in use for hosting, and what mechanisms are in place to monitor usage?

Multi-homed BGP4 routed connectivity via diverse routes over dark fibre to TeleCity Harbour Exchange and Telehouse East. For added resilience we also have cross connects with Telecity Sovereign House and Telecity Meridian Gate

What threshold is used for adding additional capacity?

The system transfer allowance is currently 10GB per month. Above this threshold, additional activity is charged to Pinnacle but no costs are passed to customers or commissioners.

What levels of authentication is used for 'trusted' companies to gain access to maintain information, i.e. will any organisation other than the Council or Supplier have the same level of visibility and access to Council data and information?

Administration of the databases and servers is by Pinnacle Health Partnership. Access to the anonymised and control information is through a single website interface which is keyed to our offices. Other levels of access are graded such that each level has access to only the information that is needed. Going upwards information is anonymised until it provides only the information required to complete relevant tasks or give an overview. Access is graded as either:
Viewer – Restricted Read Only granted by Commissioner or Restricted Read Only to a provider
Provider – Data Entry
Commissioner – Service Management

What IP addresses will be available to the Council and what are the implications regarding domain name management, both internally and externally?

The system is available at https://pharmoutcomes.org or https://outcomes4health.org, which is load-balanced between internal machines after resolution to current IP address 217.69.38.83

Will there need to be some link with our internal Domain Name System for staff supporting the services proposed?

No. This is maintained by Pinnacle Health Partnership.

Is access to servers during boot sequence available remotely?

No. Access during this phase is maintained by Pinnacle Health Partnership.

Servers

What is the server configuration?

A technical diagram is provided which illustrates the interconnectivity of the following virtualised servers utilising HA SAS RAID, managed by a Citrix XenServer Hypervisor and running on separate physical servers:

- Load Balancing OS: CentOS 5.5 with Ngnix;
- Web Server: CentOS 5.5 with Apache;
- Database Server: CentOS 5.5 with MySQL 5x; and
- Storage Server CentOS5.5 with ClamAV protection.

Who is responsible for server configuration and management, such as server OS build, application of security patches; remote server reboot or service restart, loading software, etc?
In order to manage the servers effectively and with the appropriate technical skill-set, Pinnacle Health pays for a "Total Care" managed service from Tollon Ltd, which includes Critical Server Patching, Service packs, 24 x 7 Server Monitoring and Technical Support, System Monitoring including uptime ping check, CPU usage, and disk space usage. The server configuration and management noted above therefore, managed and monitored by Tollon Ltd, Suite 4, Scotts Sufferance Wharf, 1 Mill Street, London SE1 2DE on our behalf.

Resilience

What resilience features are configured on the servers, such as hardware redundancy, load balancing, failover, clustering or shared storage like SAN or NAS?
The systems are Citrix XenServers on HA SAS RAID. They are configured to run on different physical machines in virtualised format. The hosting environment is built with a High Availability configuration such that, if one hosting server fails or experiences problems, the hosted virtual servers are automatically moved to a new host. The server configuration is currently seven servers – two providing load-balanced direction, two webservers with scripted replication and two database servers with SQL replication of the database server to the database master. A seventh machine provides both storage for documents that require virus check and computational power for calculations such as QRISK2 and JBS2. Failover is handled by the LB-HA machines, redirecting where necessary incoming and outgoing traffic. The storage unit supporting the environment are configured in RAID . The system is monitored 24x7 by both Tollon and the hardware vendor. All alerts on the system are raised to the duty engineer and the hardware vendor and an engineer is sent to the side to investigate/repair.

What pro-active management features are in place to alert on detection of a failure, and can this include alerting Council staff through a System Centre Operations Manager (SCOM)?
The system has 24/7 monitored management with first port of call for downtime out of hours of more than ten minutes to two of the partners. Similarly, any software issues are flagged by email to the partners immediately. Any issues that will fall out of our Standard License Agreement terms of downtime can be flagged to a nominated individual if required. The downtime for the first year of operation was 52 minutes in total overall through software and zero through hardware.

What levels of out of hours support is provided on these servers, both hardware and software and what are target incident fix times?
Our arrangements provide us with escalating measures in the event of incident fix times not being met that commences at four hours from identification. That is provided for on a 24 hour basis.

Pinnacle Health Partnership LLP
Weatherwise Building, Well Road
East Cowes, Isle of Wight PO32 6SP
Tel: 01983 216699 Fax: 01983 210914
www.phpartnership.com
info@phpartnership.com

Are there set standards for log file storage and reporting?
In accordance with usual operating system protocols, server log files are deleted on rotation through 28 day periods. System Audit files are removed from the system monthly, one month in arrears, and archived securely for a period of 10 years.

What configuration, change or support incident information is retained on these servers?
Tollon Ltd has ISO27001:2005 accreditation so a management and audit trail is available for all changes

What software and hardware is used to backup servers & databases?
R1 Soft Backup and R1 Soft Offsite Backup over TCP/1167 BCP with RSA & Blowfish

What is the frequency of these data backups?
10 x 4 hourly + 7 x Daily per week

What is the retention period of these data backups?
Seven days

What is done by the Pinnacle Health to verify the success / failure of these backup operations?
No direct access is provided to backup/restore functionality to the Council. Pinnacle receives a restore image once a month which is verified and actively restored on a secondary server to assure the disaster recovery process detailed later.

What records are maintained for the backup operations, and what media handling / storage provision is in place?
The R1 Solution used maintains a full audit log of active backup operations and restore requests and delivery. In accordance with usual operating system protocols, server log files are deleted on rotation through 28 day periods. The storage system for all the backup servers is on fully-monitored RAID5 systems with hot spare disks with automatic switching.

What is the process for the customer to request retrieval of information from these data backups, and would there be any additional cost for this service?
Data backups are only used for system failures and will be restored with no additional costs to the customer.

Security

What main and secondary firewall arrangements are in place and what control does the Council have over their configuration?
Tollon utilises twin redundant firewalls on the public facing interface of the network. In addition, the servers are configured with IPtable restrictions. There is no customer control available over the configuration of the Tollon firewalls. Changes to the IPtables can be requested through a support ticket by Pinnacle Health.

What happens if the Council requires a service to be allowed through the firewall which contravenes the Supplier's security policy?
This facility is not available to the Council.

What measures are in place to protect the Council's information from being compromised by the Supplier's staff, on servers as well as on backups?
Pinnacle Health Partnership Staff have secure logins with passwords which are changed monthly. Staff usage is monitored and strict confidentiality and information governance policies are followed in line with our ISO27001 accreditation

What regular measures are taken to validate security?
The system is built on object-oriented principles. The prevention of escalation penetration is our first priority when developing the system. We undertake penetration testing through First Base Technology twice yearly. The system detects a variety of intrusion triggers, all of which result in notification of the partners. Penetration testing indicates that these are effective.

What arrangements are in place to ensure privacy of information contained within the system, including any monitoring, interception or interference with information stored or passing through the system?
All access to the system is through secure HTTPS with a minimum encryption of 128bit. System level access for the partnership is through a secure VPN. The system detects a variety of intrusion triggers, all of which result in notification of at least two partners within Pinnacle Health. Penetration testing indicates that these are effective.

What contingency measures are in place to ensure continued protection and security of the customer's access to the hosting centre environment?
The customer will not have any access to the hosting centre environment.

Infrastructure Protection

What measures are in place to physically protect the hosting centre environment?
There is three stage fire detection, utilising aspiration first stage for zoned HVAC control to maximise the efficiency of the double knock addressable analogue system. A nitrogen charged 'cold-steam' independently zoned fire suppression system is discharged as a final stage. The data centre is not located in an area which has any risk of flooding. The air conditioning system is configured with 133% built-in redundancy. Effectively, only 75% of the air conditioning units are required to support the data centre at maximum occupancy. The data centre is situated on a major multi-carrier fibre route with multi-carrier bandwidth. There is a 2 megawatt on-site substation with diverse power feeds to substation and dual AKSA 1.6 megawatt generator connected via C&N ATS systems. All main switchgear can support 133% of maximum load in a fully operational data centre. 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 loads and are refuelable in use.

Pinnacle Health Partnership LLP
Weatherwise Building, Well Road
East Cowes, Isle of Wight PO32 6SP
Tel: 01983 216699 Fax: 01983 210914
www.phpartnership.com
info@phpartnership.com

What measures are in place to protect against unauthorised access to the hosting centre, and are any logs maintained of physical and/or virtual access?

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 colour CCTV. Security coverage spans from the heart of the facility to the outer compound. Data centre located inside its own secure compound with 3-metre fencing and electric entry, including anti-tailgate systems. Secure entry is via swipe card system, with 6-layer entry.

Are any regular contingency tests performed?

The hosting service is accredited to ISO27001 standards and these procedures are in place to maintain that accreditation.

Pinnacle HEALTH PARTNERSHIP

Pinnacle Health Partnership LLP
Weatherwise Building, Well Road
East Cowes, Isle of Wight PO32 6SP
Tel: 01983 216699 Fax: 01983 210914
www.phpartnership.com
info@phpartnership.com

THE BRITISH ASSESSMENT BUREAU

Est. 1969

We'll make you stand out...

The management system of

Certificate Number 197419

Pinnacle Health Partnership LLP

Second Floor, 86-88 High Street, Newport, Isle of Wight, PO30 1BH

has been assessed and certified as meeting the requirements of

ISO 27001:2013

for the following activities

The provision of software solutions for pharmacy and health care providers

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

Valid from 12 December 2015 until 11 December 2018

Authorised by

Chief Executive
The British Assessment Bureau
www.british-assessment.co.uk

UKAS MANAGEMENT SYSTEMS
8289

FSC

Certification is conditional on maintaining the required performance standards throughout the certified period of registration
The British Assessment Bureau, 30 Tower View, Kings Hill, Kent, ME19 4UY

Certificate of Assurance

Pinnacle Health Partnership LLP

1st Floor, Weatherwise Building
Well Road
East Cowes
PO32 6SP
Scope: Whole Company

Complies with the requirements of the Cyber Essentials Scheme

Date of Certification: 2nd February 2016
Recertification Due: February 2017
Certificate Number: IASME-A-00656
Profile Published: April 2014

Certification Body: baigent's Information Security Services Ltd

Assessor: Jon Baigent

Accreditation Body: IASME Consortium

This Certificate certifies that the organisation named was assessed as meeting the Cyber Essentials implementation profile published in April 2014 and thus that, at the time of testing, the organisations ICT defences were assessed as satisfactory against commodity based cyber attack. However, this Certificate does not in any way guarantee that the organisations defences will remain satisfactory against cyber attack.

Pinnacle HEALTH PARTNERSHIP

Pinnacle Health Partnership LLP
Weatherwise Building, Well Road
East Cowes, Isle of Wight PO32 6SP
Tel: 01983 216699 Fax: 01983 210914
www.phpartnership.com
info@phpartnership.com

PharmOutcomes®

Disaster Recovery and Business Continuity

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 ISO27001:2005 accredited data centres in England operated by Tollon Services 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 server in the data centre. The system is backed up live to another data centre every four hours on an incremental basis and a full system backup taken each evening. In the event of a disaster, primary user access will be switched to the secondary backup system within 2 hours.

The whole of the business continuity arrangements are subjected to a complete crash test check every year (or whenever the infrastructure changes that makes verification appropriate).

Pinnacle HEALTH PARTNERSHIP

Pinnacle Health Partnership LLP
Weatherwise Building, Well Road
East Cowes, Isle of Wight PO32 6SP
Tel: 01983 216699 Fax: 01983 210914
www.phpartnership.com
info@phpartnership.com