THE UNIVERSITY of York

PCMIS
improving patient wellbeing

# Security and Data Protection Document

# PCMIS©

## Patient Case Management Information System

# 1 Document Control

## 1.1 Document Information

| | |
|---|---|
| ***Title*** | PCMIS Security and Data Protection Document |
| ***Version*** | 2.3 |
| ***Status*** | Published |

## 1.2 Key Personnel

| | |
|---|---|
| ***Authors*** | Byron George (BG) |
| ***Reviewers*** | Ian Cope (IC), Chris Jones (CJ) |
| ***Contributors*** | University Data Centre Manager (SW) |

## 1.3 Document History

| ***Version*** | ***Date*** | ***Details*** | ***Initials*** |
|---|---|---|---|
| 1.0 | March 2013 | Initial draft | BG |
| 1.0 | March 2013 | Reviewed | IC |
| 1.0 | March 2013 | Minor amendments, reviewed | SW |
| 2.0 | April 2014 | DPA amendments, reviewed | BG |
| 2.1 | June 2015 | Reviewed | BG |
| 2.2 | January 2017 | Minor amendments, reviewed | BG |
| 2.3 | April 2018 | Annual Review, HSCN topology updated | BG |

# PCMIS IAPT System Security Document

## 1. Information Governance Compliance

PCMIS system processes, security and infrastructure are approved by the NHS Digital and the Information Governance Toolkit (IGT).
The IGT enable organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction, providing IG assurances to NHS Digital as part of the terms and conditions of using national systems and services including HSCN/N3.
Our ODS (NACS) code is 8HL30.

PCMIS is also Cyber Essential accredited https://ces.apmg-certified.com/PublicOrgLogin/Certificate.aspx?g=325567b1-bc71-44f8-ab71-356fa47823f6

## 2. Data Protection Act

The University of York is a registered data controller under the terms of the Data Protection Act, registration number is Z4855807.
PCMIS is a data processor and the ownership of any data entered onto PCMIS by the service, remains with the service. Only the named service will have access to this data. PCMIS will not process any data unless requested by the service.

PCMIS is designed to ensure no information to identify a specific patient is made available to anyone not directly involved with that person's Health. The University of York and the Department of Health Sciences do not have access to any of the data held within PCMIS, except for specified PCMIS support staff above to assist support queries.

## 3. Application Software

Data is input directly on to the Web based PCMIS System. Access is via the N3 JANET Gateway. Patient identifiable data is entered when a new case is created. The Case Number, Surname and Date of Birth are visible when using managing cases. PCMIS allows entering of fully anonymous data if required.

The Server is run on a Microsoft Windows Platform, configured to auto-update security patches on a 24 hourly basis. Anti-Virus is installed and configured to auto-update every 4 hours. Windows Backup software is used to perform full nightly backups to tape.

All data transmitted between the user and the server is encrypted using high grade TLS/SSL web based secure certificate.

## 4. Hardware

The PCMIS application is hosted on a Multi-Core, Multi-Processor Enterprise Level Server with RAID disk storage, encrypted backup tape unit, redundant power supplies, with 24 hour onsite UPS backup power. The server is subject to the manufacturer's level 1 on-site warranty. There is an onsite spare DR (Disaster Recovery) server available for immediate business continuity.

## 5. System Management

| System Responsibility | Name | Access to Confidential Data | Role |
|---|---|---|---|
| **IT Manager** – Overall responsibility for data security with Dept. of Health Sciences, University of York | Mr Byron George<br>Area 3,<br>Dept. of Health Sciences,<br>Seebohm Rowntree Building,<br>University of York<br>YO10 5DD | Yes | PCMIS Director<br><br>Dept. of Health Sciences,<br>University of York. |
| **System Developer** – responsible for technical aspects of system development. | Mr Colin Robson<br>PCMIS Development Team<br>Area 3,<br>Dept. of Health Sciences,<br>Seebohm Rowntree Building,<br>University of York<br>YO10 5DD | Yes<br>Yes | PCMIS Senior Sys Developer<br>PCMIS Dev/System Support<br>Dept. of Health Sciences,<br>University of York. |
| **Support Desk** – help desk support for Database | Mr Andrew Bradley<br>Mr Chris Jones<br>PCMIS Support Team<br>Area 3,Dept. of Health Sciences,Seebohm Rowntree Building,University of York<br>YO10 5DD | Yes<br>Yes<br>Yes | PCMIS Account Manager<br>PCMIS Business Analysis<br>PCMIS Support<br><br>Dept. of Health Sciences,<br>University of York. |
| **Data Managers** – responsible for managing supervision of case data (Supervisor) | <Supervisor List> | Yes | Service Leads,<br>Data Managers,<br>Project Managers,<br>Admin Resource Manager,<br>Counsellors, CBT. |
| **Data Users** – responsible for inputting of data (Mental Health Worker) | <Worker List> | Yes | Mental Health Workers, CBT, Counsellors. |

## 6. Data Collected

The data collected and stored within PCMIS includes patient identifiable information when entering a new case. PCMIS allows entering of fully anonymous data if required.

Fields available on the 'Add New Case' screen include:

Case Number (two letters and four digits)
Referral Date
NHS Number
Date of Birth
GP Name
Mental Health Worker Name
Worker Profession
Title
First Name
Middle Name
Last Name
Nationality
Address (Street, Town/City, County, Postcode)
Telephone Number (Home, Mobile, Work)
Gender
Disability
Sexuality
Ethnicity
Referrer
Date of Onset
Primary Referred Problem
Secondary Referred Problem
Notes.
Family Name
Previous Name
Responsible Commissioner
Previous Address (Street, Town/City, County, Postcode)
Carer's Name
Carer's Telephone Number (Home, Mobile)
Single Occupancy
Marital Status
Mobility
Main Language
Date of Death
Alerts
Email Address

## 7. Risk Assessment

A risk assessment has been carried out by the IT Manager.

| Risk | Description | Impact | Likelihood | Actions taken to minimise Risk |
|---|---|---|---|---|
| Breach of confidentiality | Deliberate “hacking” into server. | Medium | Low | All Servers are protected by an E3 compliant firewall. |
| Breach of confidentiality | Accidental disclosure of information. | Medium | Low | Access to confidential information is controlled by user authentication and role based group access. |
| Unauthorised user authentication | Disclosure of username/password. | Medium | Low | Each authorised user has an individual user account. Account management and security is available to named site supervisor. |
| Loss of data | Loss of server through fire, theft, flood, accidental or deliberate damage. | Medium | Low | Physical security of the Data Centre includes pre-authorised proximity card access to both the Data Centre and server cabinet. The cabinets are locked and have electronic audit control. The building has active fire suppressant, leak detection systems. Every walkway and cold aisle containment POD is covered by CCTV and 24 hour onsite security. |
| Loss of data | Loss of data due to | Medium | Low | Access to |

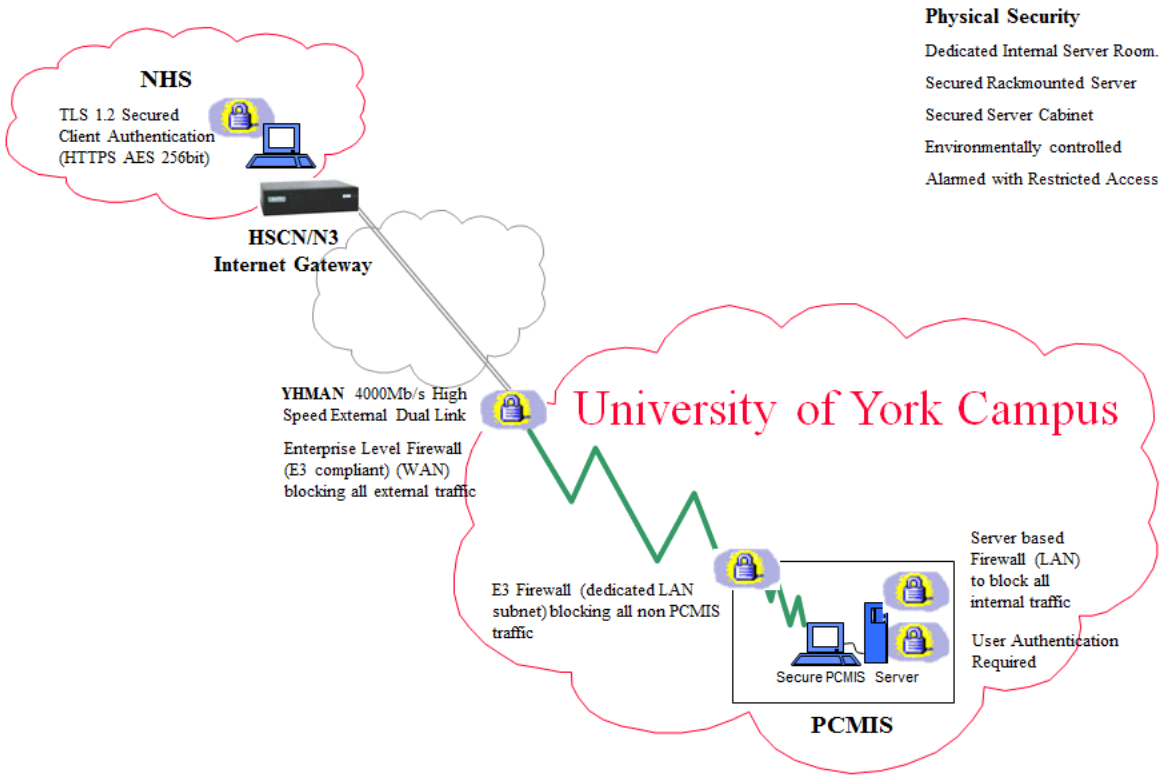
| | | | | |
|---|---|---|---|---|
| | corruption or accidental deletion | | | information is controlled by user authentication and role based group access restricting widespread corruption or deletion. Encrypted nightly backups are undertaken with active backup tape verification. |
| Loss of data | Loss of data due to corruption or theft of backup tapes. | Medium | Low | Backup tapes are AES-256 encrypted and stored in a pin-code secured, protected fireproof safe requiring authorised swipe card access. The safe is in a separate building/fire zone to the servers. Verification of data integrity is performed after each backup. |
| Data Centre power failure | Power failure preventing access to data but not destroying data. | Low | Low | The Data Centre has power redundancy in the form of UPS systems and onsite auto-start power generators. The generator has a 24 hour fuel tank and refuelling contract in place. |
| Server power failure | Power failure preventing access to data but not destroying data. | Low | Low | Each server has built in redundant power supplies and onsite next day manufacturers' |

| | | | | |
|---|---|---|---|---|
| | | | | warranty. Multiple failover hosts are available for virtual servers. Onsite cold spares are available for physical servers. |
| Failure of network perimeter firewall | Failure of firewall preventing access to data but not destroying data. | Medium | Low | Onsite cold spares are available, copies of configuration files are stored locally in a secure location. |
| Failure of the Network | Either local network failure or wide area network failure. | Low | Low | The wide area network has an active dual failover network connection, local network failure is covered by network redundancy and onsite spares. |
| Failure of server hardware | Server failure preventing access to data but not destroying data. | Low | Low | Multiple failover hosts are available for virtual servers. Onsite cold spares are available for physical servers. |
| System vulnerabilities | Breach or disclosure of information due to system vulnerability. | Medium | Low | All servers are protected by E3 compliant firewall and configured to receive automatic system updates and anti-virus software. |
| Failure of the Software | Preventing access to data but not destroying data. | Medium | Low | Encrypted nightly backups are undertaken to allow for full data restores. |

## 8. Data Transmission

All data is saved directly to the PCMIS server via a web page user interface. No data is stored on local desktop PC's. All data entered is encrypted between the PC and Server using a high grade TLS 1.2 web based secure certificate.

## 9. Access Control




**Schematic illustrating the implemented security and network layout for PCMIS IAPT Server using HSCN/N3 Gateway**

**Access to data is controlled by six levels of security.**

1. **Level 1 – User Authentication**

   Only users specified in section one, are registered with a valid username and password. Valid authentication using these credentials is required to access any data.

2. **Level 2 – Local Server Firewall**

   The PCMIS Server is protected by a local server based firewall, blocking all *internal* LAN traffic, permitting external traffic originating from the HSCN/N3 Network only (Secure https port 443 only).

3. **Level 3 – Local Dedicated Subnet Firewall**

   The PCMIS Servers are connected to a dedicated isolated internal subnet and protected by a Checkpoint hardware firewall, blocking all non PCMIS traffic, permitting external traffic originating from the HSCN/N3 network only (Secure https port 443 only).

4. **Level 4 - External WAN Firewall**

   The PCMIS Server external access is protected by an enterprise level firewall (E3 compliant), blocking all traffic, except for secure connections i.e https port 443 only.

5. **Level 5 – TLS/SSL Encryption**

   All data entered is transmitted securely, by using a high grade Secure Socket Layer TLS 1.2 (i.e. https). The data is transmitted using NHS Connecting For Health approved cryptographic algorithms guidelines, (Document Record ID Key NPFIT-FNT-TO-IG-GPG-0004.01). Weak encryption is disabled.

6. **Optional – TLS/SSL ODBC security**

   For services selecting the optional PCMIS ODBC connectivity, high grade encryption is enabled for this connection. The PCMIS Servers will only permit external connections originating from the HSCN/N3 network.

## 10.Data Backup

Full backups of the PCMIS Application Database are performed daily, both the disk and to separate rotational Monday to Thursday tapes, and five rotational Friday tapes. Hourly transactional logs are undertaken during working hours. A full system backup is undertaken weekly. Both the disk and the tape backup sessions are AES-256 bit encrypted/passwords protected. Backup media is stored in a locked fire proof safe in a separate alarmed location. Data backups are located separately by more than 5km from the live data. Only named individuals, as above in section 2 – IT helpdesk and IT Manager have access to these tapes.

## 11.Backup Data Retention

Disk backups are overwritten on a weekly basis. Tape backups are retained for 12 months stored within a locked fire proof safe in a separate alarmed location. Backup media is located separately by more than 5km from the live data. Only named individuals, as above in section 2 – IT helpdesk and IT Manager have access to these tapes. The tapes are physically destroyed in house after 12 months.

## 12.Business Continuity

In the event of any failure of any part of the system, Department of Health Sciences IT section will identify cause of the failure, and take any necessary actions to resolve the failure. Failover and redundancy is used to minimise the risk of downtime (see section 7).

## 13.Disaster Recovery

In the event of disaster recovery, every step with be taken to restore the service to operational state, by restoration of data from tape, relocation of service to the DR server, and relocating the server to a second onsite secure data centre if needed.