| | |
|---|---|
| **Reference Number:** UHB 421<br>**Version Number:** 1.1 | **Date of Next Review:** 20th Sep 2019<br>**Previous Trust/LHB Reference Number:** Trust ref 133 |

# INFORMATION TECHNOLOGY SECURITY OFF SITE MOBILE COMPUTING PROCEDURE

## Introduction and Aim

This document is written in support of the Information Technology (IT) Security Policy. It provides a mechanism to achieve and maintain appropriate security arrangements in respect of Cardiff and Vale University Health Board's (the UHB's) IT systems that hold confidential and sensitive patient and business information.

The IT Security procedure of the UHB is to ensure the safety and security of all UHB IT systems, software and in particular the UHB's Network so as to produce a safe and secure environment in line with NHS and statutory policies and procedures. This document provides further information as to the detail of the policy and its supporting information.

## Objectives

- Successful implementation of this procedure will address business and performance standards for example the requirement to meet Caldicott standards, Health and Care Standards (2015)
- Aspire to meeting BS7799/ISO27001 standards and the Information Governance Toolkit Standards as far as possible in the Welsh context.

## Scope

This procedure applies to all of our staff in all locations including those with honorary contracts.

| | |
|---|---|
| **Equality Impact Assessment** | An Equality Impact Assessment has been completed for the overarching IG and IT Policies. The assessment found that there was some impact on the equality groups mentioned in relation to communication. An action plan has been developed to address those areas. |
| **Health Impact Assessment** | A Health Impact Assessment (HIA) has not been completed. Not Required. |
| **Documents to read alongside this Procedure** | Information Governance Policy<br>Information Technology Security Policy<br>Information Risk Management Procedure<br>Electronic Incident Reporting Guide |
| **Approved by** | Information Governance Sub Committee |
| **Accountable Executive or Clinical Board Director** | Executive Director of Therapies and Health Science |
| **Author(s)** | Richard Williams (IT Security)<br>Ann Morgan (Information Governance) |

**Disclaimer**

**If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.**

**Summary of reviews/amendments**

| Version Number | Date of Review Approved | Date Published | Summary of Amendments |
|---|---|---|---|
| 1 | 20/09/16 | 28/08/18 | Reviewed and updated into new UHB format with no significant changes. |
| 1.1 | 20/09/16 | 28/08/18 | Admin changes to reflect current contact details |

**Contents Page**

# 1 INTRODUCTION

## 1.1 Purpose of Off Site Mobile Computing Procedure

The purpose of the Off Site Mobile Computing procedure is to ensure that all Cardiff and Vale University Health Board (the UHB) staff who use IT devices at home, off-site or whilst mobile for UHB purposes are fully aware of their responsibilities with regard to the UHB's IT Security Policy, Data Protection Policy, and relevant legislation

This procedure applies to devices that are provided by the UHB and also Personally Owned Devices (POD) whilst they are being used for UHB purposes

The UHB has an obligation under the Data Protection Act 1998 to ensure;
**"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".**

To ensure the UHB meets this statutory obligation, the following procedure has been produced to manage and minimise the risks associated with:

- processing person identifiable data at home or off site
- processing person identifiable data on a mobile device
- maintaining the security and integrity of the UHB network and systems

**Processing**

The definition of processing is very wide and covers nearly everything an organisation might do with data.

Processing can include any of the following:

- obtaining
- recording
- sharing
- storing
- reading
- amending
- destroying

Any organisation that processes personal information for the purposes of the Data Protection Act 1998 must comply with each of the 8 Data Protection Principles

It is essential that all information systems in the UHB are protected to an adequate level from events that may jeopardise health care activities. These events may include accidents as well as behaviour deliberately designed to cause difficulties.

The purpose of the IT security procedure is to preserve:

| | |
|---|---|
| *Confidentiality* | access is confined to those with authority to view the data. |
| *Integrity* | all systems are working in the way they were intended to work. |
| *Availability* | information is delivered to the right person, when it is needed. |

## 1.2. The Need for a Security Policy and Procedures

Data stored in UHB information systems represent an extremely valuable asset. The increasing reliance of the UHB on information technology for the delivery of health care makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.

The IT Off Site Mobile Communication procedure supports the IT Security Policy which sets out the broader implications of statutory and NHS policies in related security area. Currently the most notable UK acts are:

- Copyright, Designs and Patents Act (1988)
- Access To Medical Records Act (1990)
- Computer Misuse Act (1990)
- Computer Crimes Act (1997)
- Data Protection Act (1998)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Anti-Terrorism, Crime and Security Act (2001)

This procedure sets out how the UHB will address the requirements in operational terms.

## 1.3 Scope of the Procedure

This procedure fully addresses the IM&T security requirements of the Welsh Assembly Government DGM (96)43 ‘The Protection and Use of Patient Information’, WHC (98)80 ‘The Caldicott Report’ and WHC (99)92 ‘Protecting Patient Identifiable Information: Caldicott Guardians In The NHS’, WHC (2001)47, Code of Connection and WHC(2002)36

The procedure builds on the general requirements published by Welsh Government and these are detailed below:

- The NHS In Wales Security Policy
- Baseline IT Security Standards
- NHS-wide networking Code Of Connection For NHS Organisations

The EU directive “For the Protection of Individuals With Regard To the Processing of Personal Data and the Free Movement of Such Data” was adopted on 24 July 1995.

A Data Protection Act came into force during 1998, which included manual as well as automatically processed personal data. Staff have a common law obligation to preserve the confidentiality of this information at all times both during and after their employment with the UHB has terminated.

Further advice and guidance on individual compliance with legal and UHB policy requirements can be found in the UHB's IT Security and Data Protection Policies, or by contacting IM&T IT Security or Information Governance Departments.

The security issues covered in this document include the physical security of devices, data confidentiality and the security of UHB office systems and networks.

The security advice and individual responsibilities detailed in this procedure primarily concern personal identifiable data (PID) Personal Identifiable Information (PII) and patient identifiable information(PII), however, sensitive UHB Corporate data should be treated in the same secure manner.

## 2 RESPONSIBILITIES

This procedure applies to all UHB staff who process person identifiable data (PID) using any device for work purposes whilst mobile, or off a UHB site.

If any employee is unsure about any aspect of this procedure and its application to them, they should seek advice from their line manager as failure to comply with this procedure will be viewed as a serious matter and may result in disciplinary action

### Staff must not

- Load software packages onto UHB provided PCs or laptops without authorisation from IM&T IT Security. On no account must ‘games software’ be loaded on UHB provided PCs or laptops.
- **Disclose any of their passwords** to other members of staff.
- Logon to any computer system using another member of staff’s log in details and password.

### Staff must ensure

- They always use information they have access to in an appropriate manner at all times.
- They ensure they maintain in strict confidentiality all/any information to which they have access.

### For UHB owned IT equipment and devices:

- they have their line managers authorisation to use devices off site

- they take all reasonable steps to ensure the security of devices
- no person other than UHB staff uses the devices
- that any device taken off UHB sites is fully encrypted.
- ensure that devices are regularly returned and physically connected to the UHB IT network to maintain up-to-date anti-virus protection and security patch updates on a monthly basis. Devices not seen on the network for more than two months will have their access rights cancelled.
- where devices are used by more than one person, separate unique user National Active Directory Exchange (NADEX) ID's (Log in details), password and profiles are used.

- when devices are no longer required or staff leave the UHB employment, the devices must be returned to the relevant line manager as they are responsible for contacting the IM&T IT Security with regard to any person identifiable data stored on the device and to ensure that the user's NADEX log-on ID is removed from the UHB network.

**For UHB owned IT equipment and personal devices:**

- data must be saved to network servers and not to the local device hard drive
- when computer devices are left unattended they must either be switched off, user logged off or the screen is locked

## 3. CONNECTIVITY

The UHB uses software technology to enables users access to browse clinical and business applications from UHB owned devices and PODs.

The UHB owned and PODs that are authorised to access browser applications will have the same system access rights 'off-site', subject to any technical software application limitations.

However, use of mobile media must be signed off by managers and staff with the use to be reviewed at least annually. Mangers should also give consideration to staff undergoing additional training and staff must sign to say they've read and understood all the associated policies relevant to this.

### SMART Mobile Telephones and Tablets

- The UHB has software technology provided by Good for Enterprise, Cisco Integrated Security Engine (ISE).

- Access to the Microsoft Unified Access Gateway (UAG) software technology is provided and managed by National Information Wales Service (NWIS).

- The Good for Enterprise, ISE and UAG software is configured to only enable "downloads" into an encrypted area on the users SMART mobile telephone or tablet.

Personal Identified Information or Business Critical Information cannot be stored on PODs without the use of Good for Enterprise.

The authorisation for a user to access this service is via http://helpdesk/help/ and selection of the "Home and Mobile Working Services" icon then "The Mobile System" button.

**PCs and Laptops**

- UHB owned device connections, other than from a UHB site, will be via Thin Client Citrix Farm using 'NWIS secure ID Token or subsequently by any future UHB approved connection process.

- The Citrix Farm is not configured to allow downloading of files to local drives, even those that are encrypted

- No Personally owned PC or laptop will be allowed connection to the UHB network

The authorisation for a user to access this service is via http://helpdesk/help/ and selection of the "Home and Mobile Working Services" icon then "The Home Working System" button.

## 4. INTERNET USE

Internet e-mail services of any sort are not secure and should not be used to send person identifiable data (PID) or person identifiable information (PII).

Should the e-mailing of PID/PII be necessary this can be achieved by either encrypting the documentation with a password, to be sent in a separate email, or through the Secure File Share Portal (SFSP) system hosted by NWIS. Further information on SFSP is available via the IT Security Manager at CV.IMT.Security@wales.nhs.uk.

Please refer to the All Wales Policies for e-mail and internet use.

## 5. PERSONAL IDENTIFIABLE DATA

The following conditions apply to all devices and media, whether used on or off a UHB site:

- staff are responsible for taking reasonable steps to maintain the security and integrity of person identifiable data that is processed on a device. Non-UHB staff must not be allowed to view or access the data.

- sensitive personal data must always be saved to UHB networked servers. Sensitive personal data can only be saved to device local drive's provided that the local drive has been encrypted with the UHB's approved encryption product. Sensitive personal data saved to encrypted local drives must only be temporary and not stored long term.

- sensitive personal data can only be saved to encrypted UHB PCs, UHB laptops, mobile devices and/or media. Encryption must be with the UHB's approved encryption product. Sensitive personal data saved to encrypted devices or media must only be temporary and not stored long term.

- mobile devices should be backed up as often as is reasonably practical in line with the Service requirements, if data is stored locally. Mobile devices should only be backed up to UHB secure resources.

## 6. USE OF AGGREGATED DATA

Aggregated data tables may be used at home or off-site as this policy applies to person identifiable data and not to anonymised data.

If you intend anonymising data, prior to use at home or off-site, you must do so in compliance with the Data Protection Principles, as set out in the UHB Data Protection Policy.

## 7 PHYSICAL SECURITY

- when staff remove UHB devices and data from UHB premises they are responsible for ensuring the safe transport and storage of the device as far as is reasonably practical. Whilst travelling, devices should be kept out of sight and not left unattended at any time.

- If your UHB provided device is lost or stolen staff **MUST** notify their line manager and raise an e-Datix Incident Report immediately.

- if using a device to process person identifiable data whilst travelling or in open public areas, care must be taken to ensure that nobody else can view the device's screen.

## 8. DISPOSAL

All UHB devices must be disposed of through the IT Services Department to ensure that person identifiable information (PII) resident on the device's storage device(s) is

disposed of in a secure manner and to ensure that Environmental Legislation is satisfied.

The IM&T Department checks all mobile devices before disposal in order to determine whether they are fit for reallocation.

## 9. SUPPORT

- staff using UHB provided devices that require technical support should contact their relevant IT Help Desk.

- no support is available for home/off site working outside the Help Desk hours of 9am to 5pm, Monday to Friday.

- IT Help Desk staff will not be able to visit to resolve calls off-site

## 10. COMMUNICATION

- this procedure should be given to all staff who are given authorisation to work off site or at home.

- copies of this procedure is available to all staff and can be obtained from; the UHB's intranet site, IT Security Manager or email CV.IMT.SECURITY@WALES.NHS.UK

This document is one of several that sustain the UHB's IT Security Policy and IT Security Procedure.

## Useful Contacts

**Appendix 1**

**IM&T IT Security** cv.imt.security@wales.nhs.uk

Head of IT and Strategic Planning
Nigel Lewis Nigel.Lewis@wales.nhs.uk
Tel 02920 745600

Technical Development, Network and Support Manager
Gareth Bulpin Gareth.Bulpin@wales.nhs.uk
Tel: 02920 745605

IT Helpdesks
UHW (East) IT.Helpdesk.UHW@wales.nhs.uk
Tel 02920 745073
UHL (West) Llandough.Helpdesk@wales.nhs.uk
Tel 02920 715218

**Information Governance** cav.ig.dept@wales.nhs.uk
**Including Data Protection/Freedom of Information and E-mail monitoring**

Information Governance Manager/Clinical Coding
James Webb james.webb@wales.nhs.uk
Tel 02920 743747

Corporate Governance Senior Information and Communication Manager
Ann Morgan ann.morgan4@wales.nhs.uk
Tel 02920 744870

Information Governance Co-ordinator
Denise Gulley denise.gulley@wales.nhs.uk
02920 745625

**Appendix 2**

# TERMINOLOGY

**Device**
In this procedure, computers are defined as PC's, Laptops, Smart Devices (Phones, Tablets etc) and any other electronic device capable of processing and/or storing person identifiable data. The term 'device' is used throughout this procedure to represent computers as defined above.

**Sensitive Personal Data**

The Data Protection Act 1998 defines categories of sensitive personal data, namely, personal data consisting of information as to:-

a) the racial or ethnic origin of the data subject;

b) his political opinions;

c) his religious beliefs or other beliefs of a similar nature;

d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

e) his physical or mental health or condition;

f) his sexual life

g) the commission or alleged commission by him of any offence; or

h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

**Thin Client**
Thin Client is a method where software applications and user files, such as Microsoft Word, are located on a central server and accessed by users logging onto the UHB network from their device. When logged onto Thin Client, an individual will appear to be using the software on their device in the normal way. Note, when a user is off-line files are not accessible.

**Off-Site**
Off-site, in the context of this procedure refers to a member of staff using a device at a non-UHB location.

References to working at home in this procedure should not be confused with the concept of ‘Homeworking’. Working at home in the context of this procedure refers to staff who are based on a Cardiff & Vale NHS UHB site and who may take work home (as permitted by their line manager). Staff who take work home may still have to comply with elements of the UHB’s Homeworking Policy.