National Infrastructure Strategy for NHS Wales

Version: 1.5
Status: Final draft – awaiting approval
Authors: Informing Healthcare
Date: 15th July 2009
Document Control

Document Location

This document is only valid on the day it was printed.

The source of the document will be found on the IHC SharePoint library as part of the controlled document library. The latest approved version will be made available on Informing Healthcare’s intranet and internet websites.

Revision History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Revision date</th>
<th>Summary of Changes</th>
<th>Changes marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>V 1.1</td>
<td>22nd June 2009</td>
<td>First revised version for 2009, based on original strategy</td>
<td>No</td>
</tr>
<tr>
<td>V 1.2</td>
<td>24th June 2009</td>
<td>Revised version based on comments from IHC Technical Director and Infrastructure Team</td>
<td>No</td>
</tr>
<tr>
<td>V 1.3</td>
<td>26th June 2009</td>
<td>Revised version based on comments from IHC directors and NHS Wales IT leads</td>
<td>No</td>
</tr>
<tr>
<td>V 1.4</td>
<td>8th July 2009</td>
<td>Revised version based on comments from Head of ICT, Cwm Taf NHS</td>
<td>No</td>
</tr>
<tr>
<td>V 1.5</td>
<td>15th July 2009</td>
<td>Minor revisions based on comments at IT Leads meeting. Addition of a Vision section for management, monitoring and reporting.</td>
<td>No</td>
</tr>
</tbody>
</table>

Reviewers

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date reviewed</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gary Bullock</td>
<td>Technical Director (IHC)</td>
<td>Various</td>
<td>All</td>
</tr>
<tr>
<td>Carwyn Lloyd-Jones</td>
<td>Head of Infrastructure (IHC)</td>
<td>Various</td>
<td>All</td>
</tr>
<tr>
<td>Donald Kennedy</td>
<td>Infrastructure Consultant (IHC)</td>
<td>23rd June 2009</td>
<td>1.1a</td>
</tr>
<tr>
<td>Peter Ridgway</td>
<td>IT Consultant - Infrastructure</td>
<td>24th June 2009</td>
<td>1.1a</td>
</tr>
<tr>
<td>Various</td>
<td>IHC IT Leads Group</td>
<td>24th June 2009</td>
<td>1.2a</td>
</tr>
</tbody>
</table>

Approvers

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date approved</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carwyn Lloyd-Jones</td>
<td>Head of Infrastructure (IHC)</td>
<td>15th July</td>
<td>1.5</td>
</tr>
<tr>
<td>Gary Bullock</td>
<td>Technical Director (IHC)</td>
<td>15th July</td>
<td>1.5</td>
</tr>
<tr>
<td>IHC Executive Management Team</td>
<td>IHC Executive Management Team</td>
<td>Due 23rd July</td>
<td>1.5</td>
</tr>
</tbody>
</table>
## Contents

1. Introduction .................................................................................................................................... 5
2. Setting the Scene ......................................................................................................................... 6
   2.1 National Infrastructure ............................................................................................................. 7
   2.2 Governance Arrangements ...................................................................................................... 7
   2.3 NHS Wales Policies .................................................................................................................. 8
   2.4 Associated Documents ........................................................................................................... 9
3. Overall Vision ............................................................................................................................. 10
4. Networking Services .................................................................................................................. 11
   4.1 Vision ..................................................................................................................................... 11
   4.2 Wide Area Networking .......................................................................................................... 11
   4.3 Local Area Networks ............................................................................................................. 14
   4.4 Wireless Local Area Networking .......................................................................................... 15
   4.5 Mobile Network Connectivity ............................................................................................... 16
   4.6 IP Addressing on NHS Wales Network .................................................................................. 17
   4.7 Network Cabling and Building Infrastructure ....................................................................... 18
   4.8 Internet Connectivity ............................................................................................................. 18
   4.9 Internet Domain Name Services (DNS) ................................................................................ 19
   4.10 Network Time Services ......................................................................................................... 19
5. Servers, Storage and Hosting Environments .............................................................................. 21
   5.1 Vision ..................................................................................................................................... 21
   5.2 Data Centres and Server Rooms ........................................................................................... 21
   5.3 Physical Servers ..................................................................................................................... 23
   5.4 Server Virtualisation ............................................................................................................. 24
   5.5 Storage Area Networks ......................................................................................................... 25
6. Management, Monitoring and Reporting .................................................................................. 26
   6.1 Vision ..................................................................................................................................... 26
   6.2 Management, Monitoring and Reporting of National Services ............................................ 26
   6.3 Network Management and Monitoring ............................................................................... 27
   6.4 Server Management and Monitoring .................................................................................... 28
7. Application Delivery and User Access Devices ......................................................................... 29
   7.1 Vision ..................................................................................................................................... 29
   7.2 Application Delivery .............................................................................................................. 29
7.3 Personal Computers - Desktops/Laptops ..................................................32
7.4 Printing ........................................................................................................34
7.5 Remote Access Services .............................................................................34
7.6 PDAs and Smartphone................................................................................35

8. Messaging and Collaboration Services ..........................................................37
  8.1 Vision ...........................................................................................................37
  8.2 Email Services ............................................................................................37
  8.3 Unified Messaging .......................................................................................38
  8.4 Instant Messaging .......................................................................................39
  8.5 Presence .......................................................................................................39
  8.6 Internet Use and Monitoring ......................................................................40
  8.7 Short Message Service ..............................................................................40
  8.8 Video Conferencing ...................................................................................41
  8.9 Collaboration Tools ...................................................................................42
  8.10 Internet facing information services .........................................................42
  8.11 Voice services ..........................................................................................43

9. Directory Services and Identity Management ..................................................45
  9.1 Vision ...........................................................................................................45
  9.2 User Directory Services .............................................................................45
  9.3 National Email Directory ..........................................................................46
  9.4 Certificate Services / Public Key Infrastructures .......................................47

Glossary ................................................................................................................48
1. Introduction

This document is the second edition of the Infrastructure Strategy for NHS Wales. It is one of a series of IHC strategy documents which together describe the strategy being following by the Informing Healthcare programme and its partner organisations within the NHS and elsewhere.

The strategy has been updated to reflect the following factors:

- The major organisational changes currently being undertaken by NHS Wales
- The increasing pressure on budgets expected over the next few years as a result of the current financial climate
- Increasing opportunities for collaboration with other public services in Wales to deliver better value for money and more effective IT solutions
- Increasing security requirement to prevent against loss of data, including patient identifiable information
- New opportunities resulting from changes in technologies
- Progress and updates on projects

It considers the following infrastructure technology areas:

- Networking Services
- Servers, Storage and Hosting Environments
- Management, Monitoring and Reporting
- Application Delivery and User Access Devices (PCs, etc)
- Messaging and Collaboration Services
- Directory Services and Identity Management

For each of these, the document describes the current position, the strategic aim and the proposed next steps to achieve this aim.

It should be noted that the required resources to achieve all these aims have not yet been identified. Given the financial climate, the work will be prioritised as appropriate and, wherever feasible, in collaboration with other public services. Additionally, business cases will be created, as appropriate, in order to secure the necessary funding to achieve these goals.

This document will be reviewed annually and amended as appropriate.
2. Setting the Scene

During the development of the strategy the wider healthcare context in Wales has continued to evolve. Extensive redesign of healthcare services is to be expected as the implementation of *One Wales* takes shape. It is essential that the Infrastructure Strategy can support the current situation, the intended final state and, most importantly, the transitions between the two. Furthermore, the transitions will not be uniform across Wales. This reinforces the need for an overall design that is not dependent on a particular organisational configuration.

In broad terms, the Strategy has to migrate from the current organisational diversity of infrastructure across Wales to a corporate arrangement that can meet the requirements of current and future healthcare services. It is recognised that, whilst the existing organisational infrastructures have provided a good service locally, the scale of infrastructure change required in the future will necessitate an NHS Wales approach involving extensive redesign and investment. This is of particular relevance at the moment, due to the major organisational changes that are taking place throughout NHS Wales. Failure to update the infrastructure into a more common, corporate arrangement will put at risk the IHC Strategy as a whole, and thereby the NHS Wales healthcare transformation now well underway.

The main objectives are therefore:

- Establishing a common, corporate infrastructure architecture, design and delivery programme that delivers benefits from the outset and provides the common platform for future developments and the redesign of health services envisaged in *One Wales* and *Designed for Life*
- Supporting the organisational changes which are underway at the moment
- Driving down the cost of infrastructure, by using common products and approaches and reducing any unnecessary duplication of effort
- Securing the infrastructure to help prevent any loss of data, including patient identifiable information
- Working with other public services in Wales to establish a common approach on relevant infrastructure projects. The Public Service Broadband Aggregation (PSBA) project has already laid the foundations for this.

The strategy also sets down basic principles:

- To be safe and controllable
- To be incremental by design and make best use when possible of existing infrastructure and processes
- To achieve a balance between immediate infrastructure improvement and investment in future improvements
- To allow for differing organisational priorities, opportunities, and constraints whilst migrating to national designs and solutions
- To remain valid in the face of health services redesign
- To recognise the statutory and business obligations and requirements of NHS Wales
- To be affordable.
2.1 National Infrastructure

National Infrastructure refers to the underlying hardware, software and services that are required to deliver clinical and business applications to the end users. A robust infrastructure is essential to guarantee the delivery of these applications, thereby providing the best care to patients. The scope of infrastructure is shown below:

- Networking services, including
  - Wide Area Networks (WANs)
  - Local Area Networks (LANs), including Wireless LANs (WLANs)
  - Internet connectivity
- Servers, storage and hosting environments
  - Servers, including virtualisation and storage systems
  - Data centres - the hosting environments for the servers
- Infrastructure management, monitoring and reporting tools
- Application delivery and user access devices
  - Mechanisms for delivering applications to the end users
  - Desktop PCs, laptops, PDAs, Printers, etc
    - Including the core software such as operating systems, ‘office’ applications and endpoint security products such as anti-virus products,
  - Systems that allow remote access to NHS Wales systems and services from outside the NHS Wales network
- Messaging and collaboration services
  - Email
  - Internet facing web services, such as NHS Wales web servers
  - Video conferencing
  - Telephone systems, voicemail and unified messaging
  - Mobile telephony, including text messaging (short message services)
  - Other collaboration tools, including instant messaging and presence solutions
- Directory services and identity management

Unless otherwise stated, this document encompasses infrastructure services for all NHS Wales organisations and primary care contractors.

2.2 Governance Arrangements

This section outlines the governance arrangements over the continued development and implementation of the Infrastructure Strategy.

An Infrastructure Programme Board will be established to define, manage and ensure delivery of agreed projects. The programme will become another sub-programme under the
IHC programme, sitting alongside other sub-programmes such as the Individual Health Record and the Welsh Clinical Portal Sub-Programmes.

The Infrastructure Programme Board will be accountable to the IHC Implementation Board. It will consist of representation from the IM&T leads of NHS organisations and third party suppliers where appropriate. The Board will meet at regular intervals to report on the progress of the projects within the work streams.

The programme will be structured into work-streams relating to discipline. Therefore there will be 4 main infrastructure streams:-

- Networking (including LANs, WANs and internet access)
- Enterprise infrastructure (including server, application delivery and directory services)
- Messaging, collaboration and voice (including email)
- Security (including user verification and authentication).

As the strategy moves into the implementation phase, the configuration of projects and group membership will be revised as required.

Advice and recommendations from the ‘Welsh Public Services Infrastructure and Architecture Group’ will be considered, as appropriate, during any infrastructure design work. The following groups will provide a quality assurance role for the design work undertaken by the infrastructure programme (and its work-streams) as a result of this strategy.

- The IHC technical directorate will provide the initial quality assurance of any technical design. In particular, this will be the IHC infrastructure and security teams
- The National Architecture Design Board (NADB) will scrutinise the design and technical approach to ensure compliance with the national architecture requirements
- The clinical and technical safety issues arising from this strategy will be managed through the Patient Safety Board
- The IHC IT Directors Group will also provide technical advice and guidance on its implementation

Further information on these groups can be found at the Informing Healthcare web sites.

2.3 NHS Wales Policies

The need for consistent and pervasive standards and management of the national infrastructure supports the broader vision for NHS Wales as set out in a range of Welsh Assembly Government and NHS Wales strategies and policies

- “Informing Healthcare” (2003) established the Welsh Assembly Government’s vision to transform healthcare in Wales through the introduction of tools and techniques appropriate to the information age. This led onto the formation of the IHC Programme and the concept of common ways of working with ICT across NHS Wales
- In 2005 the Welsh Assembly Government published its vision for world-class health and social care in Wales in “Designed for Life”. This strategy seeks to recast the role of all elements of health and social care in Wales and develop a more corporate approach within the NHS and with its partner organisations. The new ways of working envisaged in
“Designed for Life” will be most effectively supported by and information and communications infrastructure that is also more corporate planned and managed

- “Healthcare Standards for Wales” (2005) defined a series of standards to improve the quality of services for patients. Standard 12 requires that treatment and care “is integrated to provide seamless service across all organisations that need to be involved, including social care organisations”. Standard 25 requires information technology to also be integrated

- “Making the Connections” (2004) seeks to gain economies of scale through greater cooperation and coordination between agencies across the whole of the public sector. It envisages improvements to the ICT infrastructure across the whole of the Welsh public service to enable bodies to work together. One of the particular challenges within informatics is interfacing networks and systems between organisations. A standard approach to the design and deployment of the national infrastructure within NHS Wales will go a long way to overcome this challenge

- In 2007 the new Coalition Government agreed a programme known as ‘One Wales’ and this includes a commitment to ‘re-design the delivery of the NHS in Wales’. ‘One Wales’ strongly reiterates the policy direction stated above particularly working together in an integrated way and replacing what remained of the internal market with a collaborative model. The ‘NHS Reform Programme’ was established in late 2008 to drive the ‘One Wales’ commitments to health re-design and by October 2010, will have replaced 22 LHBs (commissioners) and 7 Trusts (providers) with 7 integrated health boards responsible for all health care planning and delivery in their respective geographical areas. The integration of organisations, horizontally and vertically and the directive to exploit efficiency opportunities afforded by national level working creates an even more compelling case for ICT infrastructure and applications to be planned and delivered via a single national strategy

2.4 Associated Documents

The following documents should be read in conjunction with this Infrastructure Strategy document.

- National Application Strategy for NHS Wales
- National Security Strategy for NHS Wales
- National Architecture Standards for NHS Wales. This can be found on the IHC website (http://www.wales.nhs.uk/ihc)
3. Overall Vision

The overarching objective of a national infrastructure strategy is to enable users to access appropriate information services from where it is required, in a common standard national approach.

To deliver this objective, the vision for Infrastructure for NHS Wales is based on a number of core fundamental principles:

- Infrastructure should be secure and, where necessary, highly available. It needs to support and contribute towards the overall ICT service continuity strategy and subsequent business continuity planning (for all services). Further information about security, including identity management, can be found in the National Security Strategy for NHS Wales.
- Infrastructure design should facilitate the current organisational changes and should not be tied to organisational boundaries.
- Infrastructure designs and implementations must be such that they drive down total operational costs and maximise return on investment. Where appropriate, schemes that ‘invest to save’ should be undertaken. National solutions will be provided where it is deemed most cost effective and efficient.
- Where appropriate, infrastructure components will be shared with other Public Service organisations e.g. The Public Sector Broadband Aggregation network.
- Infrastructure must be configured to support the new NHS Wales.
- Infrastructure should be energy efficient and must allow NHS Wales organisations to minimise their carbon footprint, in line with NHS Wales’ environmental policies.
- Infrastructure design should be configured and scalable to provide an effective solution, both now and in the future.
- Infrastructure must adhere to minimum National standards, where agreed.
- Infrastructure should allow users to access information from wherever it is needed and facilitate the secure sharing of information (where appropriate) with other public service organisations, including social care departments and the Welsh Assembly Government.
- Infrastructure must support access to systems and information for users of all abilities, including the individual needs of people with disabilities.
- Infrastructure must support, and conform to, all appropriate national policies e.g. Welsh language policy.
- Solutions should be hosted to ensure that performance and management are as effective as possible.
4. Networking Services

4.1 Vision

A data network that provides secure access to information, with an appropriate quality of service (i.e. speed, availability) to the user based on function rather than physical location. This network must be capable of supporting current and future requirements and ensure that care of patients is not compromised. In particular, resilient and highly available networks are key in the delivery of any nationally hosted services.

Additionally, over recent years, the use of the network has increased beyond simply providing networking services to computers. A number of other systems now use the network and this continues to increase. This has resulted in the network becoming an underpinning infrastructure component on which a number of other systems/services now rely. The network must be capable of supporting such systems, including: IP Telephony, Radio Frequency Identification (RFID), patient entertainment systems, enterprise wide building access control, building management systems, CCTV, paging systems and ‘nurse call’ systems.

4.2 Wide Area Networking

Wide Area Networks (WANs) refer to the network links that are used to inter-connect NHS Wales’ Local Area Networks (LANs) on different physical sites.

Current situation

There are two general classifications of Wide Area Networks (WANs):

- Organisational WANs that link sites within one NHS organisation (typically managed by that NHS organisation)
- Core NHS Wales WAN that links the organisations to each other (managed by HSW on behalf of NHS Wales)
  - Note that some organisations do not have Organisational WANs and use the Core NHS Wales WAN as the link between their sites
The migration of the Core NHS Wales WAN to the Public Sector Broadband Aggregation (PSBA) network is almost complete.

However, the overall connection speed from NHS Wales sites to the Core NHS Wales WAN varies considerably between sites. The main difference is with connections to major hospital sites. These vary from 2 Mbps to 100 Mbps. Many sites do not have a resilient connection to the Core NHS Wales WAN. This results in a potential risk to the guarantee of service.

Some sites have two or more connections into the Wide Area Network. Typically, these are sites that host two or more NHS Wales organisations and they each have an independent link to the WAN.

Resilient WAN links are in place into the national data centres

Resilient links are in place between the NHS Wales network and N3 (NHS England’s network backbone)

**Strategic aim**

- A WAN that supports rapid access to information systems, including images and video content
- High speed and resilient connections into the national data centres to support the provision of nationally provided services.
• The overall circuit connection speed, from a site to the Core NHS Wales WAN, must be equitable across sites of a similar type and size
  o These will need to be sized appropriately to support access to off-site hosted services, such as those delivered from national data centres.
  o Resilient connections to all sites that need it for business continuity
    ▪ Physical diverse routes or alternative ‘over the air’ technology (e.g. microwave) will be used to achieve this.
  o Removal of any unnecessary duplication of circuits into the same sites.
  o A common Quality of Service (QoS) policy to be implemented end-to-end across the entire NHS Wales network to support timely access to applications
  o WAN optimisation technologies to be considered to improve the end user experience as an alternative to increasing circuit speeds
• High speed internet access to support internet hosted services and e-learning for medical and other NHS staff. See Section 4.8 for further details
• High speed and secure connections to application service providers e.g. McKesson (ESR and Financial Systems).

Figure 2 - Schematic of proposed NHS Wales WAN
Proposed next steps

- Complete the migration to the PSBA network
- Create minimum standards for WAN connections to the NHS Wales Core network. This will take into consideration the following factors
  - Type of site (large/acute hospital, community/mental health hospital, community clinic, GP surgery, etc)
  - The networked applications used at the sites (e.g. PACS / imaging systems, Video Conferencing, email, etc)
  - The applications that are hosted off-site such as the new Laboratory Information Management System (LIMS)
  - Impact to the users at the site in the event of network outage.
- Upgrade WANs, or deploy WAN optimisation technologies, to meet minimum requirements
  - Note that the initial prioritisation order for these upgrades will be the sites that need fast and resilient access into order to support the new Laboratory Information Management System (LIMS).

4.3 Local Area Networks

Local Area networks are the data network(s) physically located within one site e.g. Hospital, Clinic or GP surgery.

Current situation

- Reasonably fast LANs exist in most NHS organisations to support current local requirements (typically 100 Mbps to the desktop)
- LAN connections to servers are typically 1 Gbps
- Core network speeds in large hospital sites are typically >= 1 Gbps
- Features supported on the LAN equipment (e.g. QoS, Network Access Control, Power over Ethernet) vary considerably across sites and organisations
- Resilience options also vary considerably across sites and organisations
- Designs for LANs vary considerably between sites and organisations
- There is no common vendor and as such, there is a duplication of technical skills and sub-optimal network support arrangements
- In summary, there is no minimum standard, high speed connectivity is not always available or guaranteed and the cost of support is not consistent or transparent at a national level.

Strategic aim

- Pervasive, secure network that provides high speed connectivity to the users
• A network that conforms to the national standards which will be defined in the National Architecture Standards Document

• Rationalise the number of equipment vendors, considering:
  - Value for money
  - Availability of support staff and engineering resources
  - Technology area and best of breed
  - Adherence to industry standards

• Fully resilient LANs (where appropriate) to support increasing clinical, and other, dependence on technology

• Standardised LAN configurations across NHS Wales. These should look to maximise the use of freely available networking features to increase availability, security and speed.

Proposed next steps

• During the organisational changes, assess all opportunities for rationalising equipment vendors, suppliers and support/maintenance arrangements

• Evaluate existing procurement frameworks and provide national contracts for purchase and support/maintenance of LAN equipment

• Create approved LAN standards and consistent LAN design frameworks for NHS Wales

• Carry out a baseline review of existing LAN provisions against LAN standards and strategy and confirm gaps

• Upgrade LANs to meet minimum standards.

4.4 Wireless Local Area Networking

Wireless Local Area Networking (WLAN) is a technology that allows devices (e.g. laptops or PDAs) to connect to a physical network or to each other without the use of any physical wired connections.

To support care provision closer to the patient there will be an increased dependency on wireless technologies such as WLAN. Examples of processes that could benefit from WLAN coverage, in conjunction with mobile devices, include transcribing, prescribing, and test requesting.

Current situation

• WLAN coverage is provided on an ad-hoc basis

• Use of the WLAN varies. Most organisations use the WLAN to provide connectivity to laptops; others are trialling wireless IP telephony, asset tracking using RFID, etc.

• Different designs for WLAN implementation

• Different standards are used – especially relating to security. A minimum WLAN security standards documents exists, but a common authentication method has not been chosen for NHS Wales
• Without a common approach, users are unable to roam within NHS Wales and access network services wirelessly.

Strategic aim
• Provide pervasive and secure WLAN coverage to support mobile working and be enablers for process re-design. For example, using the WLAN to enable:
  o Bedside access to the Welsh Clinical Portal functionality – e.g. medicines transcribing
  o Wireless IP telephony
  o RFID and asset tracking – Use in locating medical equipment (pumps, etc)
  o Replacement of pager systems
• WLANs to be used to supplement the fixed LAN infrastructure, not to replace it
  o WLAN can be used to improve resiliency to fixed LAN (if access point is supplied from a different wiring cabinet)
• Common, agreed WLAN designs and authentication standards across NHS Wales which will allow users with mobile devices to roam around NHS Wales organisations and connect to corporate resources over the WLAN.

Next Steps
• During the organisational changes, assess all opportunities for rationalising equipment vendors, suppliers and support/maintenance arrangements
• Evaluate existing procurement frameworks and provide national contracts for purchase and support/maintenance of WLAN equipment
• Create approved WLAN standards and consistent WLAN design frameworks for NHS Wales
• Implement a common SSID and authentication mechanism on all new and existing WLANs to allow mobile users to access network resources when they roam between sites and organisations. This will use the national CYMRU domain for authentication (See section 9.2)
• Carry out a baseline review of existing WLAN provisions against WLAN standards and strategy and confirm gaps
• Upgrade WLANs to meet minimum standards.

4.5 Mobile Network Connectivity

Within this strategy, mobile network connectivity refers to technologies such as General Packet Radio Service (GPRS) and Third Generation Networks (3G) which allow wireless connectivity to the NHS Wales Network from a wider geographical area (i.e. locations other than NHS Wales’ sites).

Please see Section 7.6 for further information on PDAs and SmartPhones.
Current situation

- There is an increasing requirement for providing network connectivity for users working in the community where there is no direct access to LAN, WAN or WLAN services e.g. to support the rural health and chronic disease policies
- There is limited use of GPRS and 3G technology in a number of pilot projects
- GPRS and 3G coverage is worst in the areas that need it most e.g. rural areas
- Some existing implementations of GPRS and 3G are not adopting best-practice guidelines for these technologies

Strategic aim

- To make best use of mobile network technologies in order to support mobile working, wherever the patient and care provider are situated. However, networking technologies can only form part of a wider solution for mobile working.

Proposed next steps

- Evaluate lessons learnt from existing pilots and publish best practice guidelines and standards for using mobile technologies
- Consider how the data portion of the AirWave voice network used in ambulances can provide data connectivity to ambulances and other mobile workers.

4.6 IP Addressing on NHS Wales Network

Internet Protocol (IP) addresses are addresses assigned to devices connected to an IP network that allows each device to communicate with each other and be uniquely identified.

Historical Situation

- IP addresses used by NHS Wales Network were in the range 130.x.x.x to 145.x.x.x. These are valid internet IP addresses, but were not registered to NHS Wales. As such, there were conflicting IP addresses which resulted in problems when NHS Wales’ users tried to access internet sites which used the same IP addresses
- NHS Wales also had IP addresses that clashed with IP addresses within NHS England

Current Situation

- NHS England (Connecting for Health / N3) have allocated a private range of IP addresses for NHS Wales (10.56.x.x to 10.71.x.x)
- NHS Wales organisations are migrating their networks and devices from the old addresses to these new addresses

Strategic aim

- To monitor the adoption of IPv6 in the UK and to plan a migration to IPv6 if/when the time is right
Proposed next steps

- Complete the migration to the new IP addresses.
- Explore the implications of migration to Internet Protocol Version 6 (IPv6) and develop an implementation plan.

4.7 Network Cabling and Building Infrastructure

This section refers to the physical wired computer network cabling that is installed into NHS buildings.

Current situation

- A significant amount of low standard legacy cabling exists (e.g. Cat 3, Cat 5, etc)
- The currently approved minimum cabling standards was created in 1999 and has not been updated.
- A draft document exists which stipulated the ‘Minimum infrastructure standards’ for new NHS sites. This is for new NHS installations into buildings (i.e. not necessarily NHS owned buildings)

Strategic aim

- Provide approved infrastructure standards for new NHS buildings, including national cabling standards for data networking.

Proposed next steps

- Produce approved infrastructure standards for new NHS buildings, including national cabling standards for data networking.

4.8 Internet Connectivity

This section refers to the data circuits and other infrastructure that provide internet connectivity for web browsing services, internet email, remote working and the hosting of NHS Wales web sites. See also sections 7.5, 8.6 and 8.10 for further information.

Current situation

- NHS Wales currently has several different circuits (with different suppliers) and associated infrastructures for internet connectivity. Most of these are managed by HSW, but there are some others managed by other NHS Wales organisations
  - Many of these circuits and infrastructures are not in a high-availability arrangement, i.e. have single points of failure
  - The infrastructure that supports the internet facing services (known as the DMZ) is several years old and needs updating
- Bandwidth on several of the circuits is insufficient for their purposes. In particular the circuits that support remote working (see section 7.5), which would be heavily used in the event of a pandemic flu outbreak
Strategic aim

- High speed internet access to support internet hosted services and e-learning for medical and other NHS staff
- A rationalised number of highly available, internet circuits and DMZ infrastructures for supporting web browsing services, internet email, remote working and the hosting of NHS Wales web sites

Proposed next steps

- Take forward the necessary actions for achieving the strategic aim. Where possible, this will be leveraging the PSBA network

4.9 Internet Domain Name Services (DNS)

A Domain Name Service (DNS) translates internet domain names (e.g. www.wales.nhs.uk) into IP addresses (e.g. 217.140.41.240).

Current situation

- Domain Name Services for resolving “.wales.nhs.uk” addresses on the internet are currently provided by BT. However, in order to provide high availability options for internet facing NHS Wales web sites, DNS servers should be under the direct control of NHS Wales.

Strategic aim

- NHS Wales host own internet facing DNS servers, thus providing a high availability option for NHS Wales hosted web sites.

Proposed next steps

Take forward the strategic aim as part for the ‘Proposed next steps’ of Section 4.8.

4.10 Network Time Services

Network time services are systems that provide time synchronisation for the various devices that connect to the data network. This includes PCs, servers, routers, switches, firewalls, etc.

Current situation

- Time synchronisation services are provided by various means within NHS Wales
- An aging time synchronisation services is hosted by HSW. This has a radio links to the ‘atomic clock’ transmitter in Rugby.

Strategic aim

- One highly available time synchronisation service hosted nationally which is used by all NHS Wales organisations
Proposed next steps

- Investigate options for providing a highly available time synchronisation service for NHS Wales.
- Procure and implement as necessary.
5. **Servers, Storage and Hosting Environments**

This section refers to secure hosting environments and associated server processing and data storage infrastructures.

5.1 **Vision**

Standardised servers, storage, virtualisation tools, management tools and processes used throughout NHS Wales, to maximise efficiency, lower costs and improve the overall service availability to the end user. This should be coupled with rationalisation of the number of hosting environments into a number of strategically located secure data centres. Appropriate upgrades to the wide area network will be required to support this configuration.

5.2 **Data Centres and Server Rooms**

For the purposes of this document, ‘data centres’ refer to large scale, fully managed and secure sites that have been custom built to house server equipment. ‘Server rooms’ refer to smaller rooms that have evolved into hosting environments.

**Current situation**

- Some larger organisations with large sites (e.g. acute hospital sites) have rationalised data centres. However, due to recent and ongoing organisational changes, these are no longer necessarily optimised for the new organisations
- Many dispersed smaller server rooms (with a few servers) also exist across NHS Wales sites and organisations
  - In some cases, where multiple organisations are located on one single sites, more than one server room exists at that site
- The current default hosting location for National Services hosted by NHS Wales is a Tier 3\(^1\) data centre facility, located in Cardiff. Where a second site is required, server rooms in Health Solutions Wales’ (HSW) premises are used
  - However, there is a limited amount of additional space in HSW server rooms and this is likely to cause capacity problems in the near future
- Some national services for primary care are hosted from Mamhilad Park in Gwent
- Some national applications are hosted by the application provider (e.g. McKesson).

**Strategic aim**

- A more rationalised approach, with consolidation of data centres, i.e.
  - Upgrading strategic data centres to meet the minimum security standards for holding personal identifiable information
  - Upgrading the wide area network to provide fast and resilient access to these data centres

\(^1\) As defined by the UpTime Institute ([http://www.uptimeinstitute.org](http://www.uptimeinstitute.org))
- Migrating services from the smaller data centres/server rooms into these secure data centres and decommissioning the unused rooms

- Data centres to be shared between organisations, especially when located on the same physical sites

- For nationally hosted services, three data centres will be used.
  - Applications will be mirrored/replicated between two of the sites. This will be achieved through true active/active deployment (where data is served from other site) or in an active/passive deployment (where the services are still resilient within one site and normally only served from that site). In this latter case, a manual failover is required to serve the services from the other site.

![Diagram of primary data centres](image)

**Figure 3 - Diagrammatic representation of the primary data centres**

- A third site will be used for storing backups and for disaster recovery purposes

- The three sites will be geographically dispersed
  - The two primary sites will need to be close enough together to have high speed and low latency network links between them to allow synchronous data replication
  - The third site should be located as far as possible away from the first two sites, but balancing this with other factors, such as wide area network connectivity costs
Figure 4 – Diagrammatic representation of the three main sites

- The network links between these data centres, and between the data centres and the PSBA network will be made as resilient as possible at reasonable costs
- Data centres to be located close to the high-speed core of the PSBA network, or the core should be re-designed to ensure that high-speed connectivity can be made available at the data centre locations

Proposed next steps

- Data centres to be rationalised and upgraded to meet minimum security standards for holding personal identifiable information. This is particularly relevant for sites that have multiple data centres for multiple organisations and for organisations that have sub-optimal hosting arrangements as a result of organisational reconfiguration.
- For sites whose business continuity requires a continuous IT service, this should primarily be achieved through resilience at the network layer rather than through duplication of data and/or services at that site. Note that all copies of person identifiable information will be need to be stored in secure data centres.

5.3 Physical Servers

Current situation

- The server systems used by NHS Wales organisations are purchased from a range of vendors
  - Understandably, actual configurations of servers vary, but there are no minimum standards for basic items like power supply redundancy, remote management options, etc.
- The server and storage solutions for IHC-delivered national services are procured from a single hardware vendor
- Typically, servers are over-specified and therefore there is a significant amount of spare processing power and storage
• Server virtualisation is fairly widely deployed within NHS Wales (See Section 5.4)

Strategic aim
• All NHS Wales organisations use servers from a selected server vendor. This will result in savings in initial purchase and on-going support costs.
  o It is acknowledged that, in some cases, there will be a need to purchase another vendor’s specific hardware in order to support highly specialised clinical and business systems.
• All servers conform to minimum specifications in order to ensure highest possible availability
  o Hardware options (e.g. power supply resilience), security standards (e.g. hardening the operating system according to best practices, etc)
• Increased use of server virtualisation and consolidated storage solutions for more effective use of available resources and to minimise the overall power consumption. See sections 5.4 and 5.5 for more details
• Common server management tools and processes for the majority of server systems in NHS Wales organisations (See section 6.4)
• Server and storage hardware and software refreshed regularly, in order to support the latest national applications and national standards

Proposed next steps
• Creation of a minimum server specification document
• Creation of a baseline server security document
• Undertake a framework procurement for a single supplier of server hardware for NHS Wales

5.4 Server Virtualisation

Server virtualisation allows multiple server operating systems (e.g. Windows Server 2008) to run on one physical server. It allows for the very efficient use of physical server resources (e.g. processing power and memory) while also providing high availability options and easier upgrade paths in the future.

Current situation
• Most organisations have implemented server virtualisation systems in order to reduce the server footprint in data centres. Some organisations have undertaken server consolidation projects, but others are taking an ad-hoc approach
• Many different server virtualisation products are currently used, but the majority of products are bought from one vendor
  o As the software licences are purchased in ad-hoc arrangements, NHS Wales is not getting best value for money. This applies for the initial purchase and for support and upgrade arrangements
Strategic aim

- Server consolidation using virtualisation being used wherever appropriate. Highly available virtual server farms will be required
- One common server virtualisation product with a national licensing and support agreement
  - It is acknowledged that vendor specific products are needed in order to support highly specialised clinical and business systems

Proposed next steps

- Undertake a framework procurement and/or national licensing arrangement for a single supplier of server virtualisation products and support for NHS Wales

5.5 Storage Area Networks

Storage Area Networks (SANs) refer to networked storage systems that allow flexible and efficient use of data storage. SANs typically provide high speed access to large, highly available storage solutions.

Current Situation

- Most servers have local storage, internal storage or directly attached storage
- Many NHS Wales organisations have implemented Storage Area Networks
  - However, differing hardware from various equipment vendors is in use
- The server and storage solutions for IHC delivered national services are procured from a single hardware vendor

Strategic aim

- Consolidation of storage onto highly available SANs
  - Use of storage virtualisation and tiered storage to maximise efficiency and minimise overall costs
- One single approved SAN vendor for use across NHS Wales
  - It is acknowledged that vendor specific products are needed in order to support highly specialised clinical and business systems

Proposed next steps

- Evaluate existing frameworks and procurement options for a single supplier of storage products for NHS Wales
6. Management, Monitoring and Reporting

This section refers to the various software tools, documentation and processes that are used to manage, monitor and report on the performance of infrastructure, applications and services.

6.1 Vision

Standardised management, monitoring and reporting tools and processes used throughout NHS Wales, to:

- Maximise efficiency and effectiveness,
- Lower costs
- Provide more consistent report on performance, availability, etc
- Improve the overall service availability to the end user

6.2 Management, Monitoring and Reporting of National Services

Current situation

- A number of management, monitoring and reporting tools are in use for national infrastructure, applications and services.
- There is no overall design, or agreed approach, for the management, monitoring and reporting for the national infrastructure, applications and services. As such:
  - Many different tools are being used to manage, monitor and report the same infrastructure, applications and services
  - The most appropriate tools are not being used in all cases
  - Many of the tools have not been fully configured or ‘tuned’ appropriately and as such are not providing the best information to the users of those tools
  - Free tools that are ‘built-in’ to existing infrastructure components are often not being used

Strategic aim

- An agreed design and approach for the management, monitoring and reporting for the national infrastructure, applications and services
- Rationalised set of tools for management, monitoring and reporting
- Appropriate tools deployed, configured and tuned as necessary to monitor and report on:
  - Individual components of the infrastructure and applications
  - Actual service levels (availability, performance, adherence to SLAs, etc) as experienced by the end users of the service

Proposed next steps

- Define service deliverables and corresponding measurements for each service
• Define a list of appropriate maintenance tools, taking into considerations
  o Investments and skills with existing tools and processes
  o Options for ‘all-in-one’ tools as opposed to multiple separate tools
• Create designs and requirements for management, monitoring and reporting toolsets based on above
• Procure toolsets and related training (if necessary)
• Deployment and configuration / tuning of the agreed toolsets

6.3 Network Management and Monitoring

Network management and monitoring refers to the tools and processes that are used to manage the computer networks (LANs, WANs and WLANs) and monitor their availability and performance.

Current situation
• Network management is a two tier model
  o Organisational WANs and LANs are managed by those organisations
  o The core WAN is managed by Health Solutions Wales (HSW) on behalf of NHS Wales
• There is no national visibility of end-to-end network availability and performance. This provides significant challenges when delivering nationally hosted services.
• The tools used to manage and monitor networks vary between organisations. The amount of knowledge and skills with these tools also varies significantly
• The documentation quality and format varies
• As a result, end-to-end network and service management is not possible.

Strategic aim
• A common toolset for end-to-end network monitoring and management. These must be capable of managing and monitoring hardware from multiple vendors
• Implementation of national end-to-end network management and monitoring solution which will integrate well with an overall end-to-end service management solution. Such tools will need to:
  o Allow local control to respond quickly to local demands
  o Be deployed in an hierarchical configuration to limit performance overhead on the overall network
• Where applicable, approved vendor specific network management tools will be used

Proposed next steps
• Design and procurement of national network management and monitoring tools
• Evaluate existing frameworks and provide procurement contract for vendor specific tools, where applicable
• Implementation of national end-to-end network monitoring solution

6.4 Server Management and Monitoring

Server management and monitoring refers to the tools and processes that are used to manage the server and storage systems and monitor their availability and performance.

Current situation

• The tools used to manage and monitor server and storage systems vary between organisations. The amount of knowledge and skills with these tools also varies significantly
  o In some cases, where different parts of an organisation manage different server services, different tools are also used

• The documentation quality and format varies
• As a result, end-to-end service management is not possible.

Strategic aim

• A common toolset for monitoring and managing server and storage systems.
  o These tools must be able to monitor the health and performance of server and storage hardware and the applications that reside on the servers
  o It is acknowledged that vendor specific server and storage management tools will be needed into the short term (while different server and storage products exist), and also in the longer term to support servers and storage provided as part of a highly specialised clinical or business application

Proposed next steps

• Design and procurement of national server management and monitoring tools
• Evaluate existing frameworks and provide procurement contract for vendor specific tools, where applicable.
7. Application Delivery and User Access Devices

This section discusses the user access devices (e.g. PCs, Laptops, Thin clients, etc) and the means of delivering software applications and services to those devices.

7.1 Vision

- Users are able to access their applications and data from any user access device on the NHS Wales network. If they move between devices, their settings and running applications will follow them.
  - They will also have secure remote access to applications, and the level of access to those applications will depend on their location and the trustworthiness of the local device (e.g. a higher level of application access would be given from a social services PC on a social services network, than from an unknown PC in a cybercafé)
- Cost savings and rationalisation of application delivery wherever possible to drive down the total cost of ownership to NHS Wales
- Where sensitive information (including patient identifiable information) is stored on the devices it will be encrypted to appropriate standards

7.2 Application Delivery

Application delivery refers to the mechanism by which computer software applications (e.g. Microsoft Word or Internet Explorer) are delivered to the end users.

Current situation

- The mechanism by which applications are delivered to end users varies across NHS Wales organisations. Some use thick clients with deployed applications and others have invested in thin client technology.
  - Where thick clients are used, a range of tools are used for installing and configuring the applications.
  - Where thin clients are used, different products and techniques (published desktop vs published application) are used.
- Most organisations do not have fully managed desktop environments, i.e.
  - One standard means of deploying all desktop operating systems and applications.
  - ‘Locked down’ desktops, preventing any configuration changes by the user
  - Roaming user desktops, and a common user experience at all devices.

Strategic aim

- A phased migration towards an internal ‘cloud’ delivery model. Figure 5 shows a diagrammatic representation of this, with a further explanation following beneath it.
With this model, the common business and clinical systems are being delivered nationally, but with organisational delivery of specialist business and clinical systems i.e.,

- Common business applications and national clinical applications delivered nationally for NHS Wales. These would be applications such as:
  - Office suites (word processing, spreadsheets, presentation software, etc)
  - File storage systems (user home space and departmental storage space)
  - Email
  - Internet browsing
  - Enterprise business applications, such as the ESR, e-KSF, procurement systems, financial management systems, etc
  - Collaboration tools
  - The new Laboratory Information Management System (LIMS)
  - The Welsh Clinical Portal
  - The Individual Health Record

There is little added value in delivering these applications locally and significant benefits can be realised by delivering nationally, such as:

- Specialist, dedicated support staff supporting these systems for NHS Wales
- Cost savings resulting from less duplication of effort across Wales
- Cost savings resulting from less duplication of systems and storage across Wales
- Facilitates providing secure access to NHS Wales applications and data for other organisation (e.g. Social Services)
  It must be noted that there would need to be an initial investment in software licences and hardware in order to achieve this
- The user access devices and specialist business and clinical systems being managed and delivered at organisational level. This allows the flexibility required during the migration to support specialist ‘local’ clinical and business systems such as
  - Legacy PAS systems
  - Legacy PACS, etc.

- A migration toward thin client devices, with virtual desktop technologies - where feasible. With this model, the user’s desktop processing and storage all takes place in secure data centres with a ‘thin’ user access device essentially comprising of a keyboard, mouse, monitor and some basic graphics processing capability. There are significant benefits with this delivery model, including:
  - Direct savings
    - Savings in electricity costs (Thin client devices consume significantly less power than PCs). They also produce less heat, so less electricity is required for air-conditioning systems
    - Thin client devices have much longer lifecycles than traditional PCs. Typically, a PC will have to be replaced twice as often than a thin client device. Thin client devices are also cheaper than PCs.
    - No need for encryption product licences as no information is stored on a thin client device
    - No need for other ‘remote support’ software licences
  - Indirect savings (in reduced management costs)
    - Less duplication of effort
    - Less visits by IT staff to support the user devices
    - Standard ‘locked down’ desktop images can be deployed, less time spend troubleshooting and fixing user created problems
    - Simpler upgrade paths to latest operating systems, as the operating systems runs in the data centre, not on the client device
  - Other benefits
    - Simpler security model as all data is stored in secure data centres
    - Roaming desktop sessions – i.e. when a user logs in to any device their desktop and running applications are displayed on that device

There are also some drawbacks with this model, including:
- This delivery model may not suitable for all applications / user devices, in particular those with requirements for high power graphics capabilities. Testing will need to be undertaken as necessary
o This delivery model is not suitable for mobile devices when they are not connected to the network, but similar technologies (e.g. desktop streaming and application streaming) can be used in the scenarios

o More processing power (and therefore electricity, cooling, etc) is needed in the data centres. However, the overall electricity draw is significantly reduced with this model.

o Additional software licensing costs

o More reliance on the data network

o The need for higher skilled staff to support the server side components with the delivery model

Proposed next steps

- Progress the work in realising the strategic aim. In particular:
  - Test the above technologies and principles in the IHC research labs or in NHS organisations that are already using similar technologies
  - Work with the vendors that provide the suitable technologies, to inform the necessary business cases.

7.3 Personal Computers - Desktops/Laptops/Tablets

Current Situation

- Hardware from various suppliers is used by different NHS Wales Organisations. Value Wales has a national procurement framework in place for such devices
  - No national minimum specification for new hardware purchased. Currently, PCs with significantly differing specifications are purchased. The majority of new PCs are specified to run Windows XP, not Windows Vista or Windows 7.

- The build process (Installation of Operating Systems, and core applications) differs across organisations
  - Various third party tools are used, although tools from Microsoft (SCCM+WDS) were included in the Enterprise Agreement

- The management tools (remote control tools, software installation tools, etc.) differ across organisation
  - Various third party tools are used, although Client Access Licences for Microsoft Systems Centre Configuration Manager (SCCM) for all devices were included in the Enterprise Agreement
  - Patch management is done on an ad-hoc basis with most larger organisations having some form of solution whilst most GP practices do not

- A range of Operating Systems are still used on PCs across NHS Wales
  - Windows 95, 98, NT, 2000, XP and Vista
  - Various Linux distributions

- ‘Core’ desktops applications differ across organisations and within organisations e.g.,
Different security tools, including encryption tools, endpoint security tools, anti virus solutions,
Different versions of Office and JAVA Runtime Environment
This diversity results in significant challenges and risks in supporting national solutions.

Strategic aim
- Standardisation across all elements of user access devices and their management
  - One vendor for all of NHS Wales, ideally for all of the public sector
  - A range of standard configurations to balance the processing needs with the environmental factors and costs
  - Common look and feel and a ‘slick’ roaming experience
    - If a user uses a different PC within the same organisation, or in a different organisation, it will look very similar to their usual PC and no additional configuration will be required (e.g. setting up Outlook or mapping network shares and printers)
    - Common Operating Systems and core applications deployed on all PC. This reduces the management overhead and testing requirements when deploying new applications
      In practice, while applications are deployed directly onto PCs, there will be some slight variation between PCs as different application versions will be used in order to deal with the various ages of PC hardware and diversity of applications
  - Common build, management tools and processes across all NHS Wales organisations
    - A National Windows Update Services server and/or BITS (Background Intelligent Transfer Service) compliant cache to facilitate with the patching of Windows operating systems
  - Device configurations are optimised to minimise their power utilisation
  - Hardware refreshed regularly, in order to support the latest national applications.
  - Operating systems and other infrastructure software to be refreshed regularly to ensure that they are covered by main stream support solutions from the software suppliers. Where this is not possible, alternative support arrangements will need to be established.

Proposed next steps
- A national procurement for all PCs, Laptops and Netbooks for NHS Wales
  - A range of standard configurations and upgrade options to be included
  - Additional ‘value added’ services to be included (e.g. installation and configure services)
- Design common build, deployment and management tools/methodologies for all NHS Wales.
o Investigate options for facilitation the common look and feel and ‘slick’ roaming experience
o This piece of work to be linked to ‘Proposed Next Steps’ in Section 7.2

7.4 Printing

Current situation
• Some NHS organisations have ad-hoc printing arrangement – few networked printers and many desktop printers. This has a total higher cost of ownership and is not a very energy efficient solution.

Strategic aim
• Optimised printing services in all NHS Wales organisations.
  o Highly available networked printing services used where possible, but locally attached (and mobile) printers used where appropriate
  o Energy efficient solutions
  o Lowered total cost of ownership.
• Rationalised number of printing vendors
  o One vendor for all standard printing solutions (regular A4 / A3 printing)
  o Other vendors, as required for specialist printing solutions (Bar code printers, sample bag printers, etc)

Proposed next steps
• Investigate networked, locally attached and mobile printing services with the major printer manufacturers
• A national procurement for standard printing solutions

7.5 Remote Access Services

This section refers to those systems and technologies that allow users to access NHS Wales’ resources securely from the internet and other third party networks (e.g. Social Services).

Current situation
• NHS Wales has three supported solutions
  o An IP-SEC VPN solution. This allows users with NHS Wales owned and managed computers to tunnel securely over the internet and obtain access to their organisation’s resources directly from those computers
  o A Secure Application Publishing Gateway. This allows users with NHS Wales owned and managed computers to tunnel securely over the internet and obtain access to their organisation’s resources using a Thin Client Solution. Some NHS organisations allow users to connect to this gateway from home PCs, but only after following approved (and audited) security procedures
o A dial up solution. This allows users with NHS Wales owned and managed computers to connect securely over the Public Services Telephone Network (PSTN) and obtain access to their organisation’s resources directly from those computers

- Two factor authentication is used with all solutions, in order to provide stronger authentication
- These services are not fully resilient and are only supported during the working week

**Strategic aim**

- Highly available and secure remote access services which provide access from both NHS owned / managed devices and other devices (e.g. home PCs, cybercafés or PCs belonging to other public sector organisations).
  - This will be linked to the application delivery solutions described in Section 7.2
    - Access to applications will depend on the location that the user connects from, e.g. if a user connects from a social services site, they might have access to more applications that if they connect from a cybercafé
    - Can provide a fallback option (when combined with a mobile internet service) for critical users in the event of a WAN failure to a site
  - A secure and auditable solution will be included to providing secure access to suppliers over the internet
- A range of two factor authentication options to be linked to the above

**Next Steps**

- Progress the work in realising the strategic aim. In particular:
  - Upgrade or replace the Secure Gateway solution to support secure access to users from home PCs. This would be particularly useful in providing flexible working options in the event of a pandemic flu outbreak
  - Testing additional two factor authentication options

**7.6 PDAs and Smartphone**

Personal Digital Assistants (PDAs) and Smartphone refer to the personal electronic devices that can store and process information including email, contacts, calendars, etc. Both classes of devices now commonly come with integrated mobile phones and mobile network connectivity capability (See Section 4.5)

**Current situation**

- There are a mix of:
  - Secure managed devices, e.g. BlackBerry
  - Unmanaged devices (various phones, PDAs and other similar devices) that synchronise emails, contacts, calendars, files, etc

**Strategic aim**
• One single secure and fully managed solution for providing mobile access to users, which supports a variety of mobile devices and carriers.

**Next Steps**

• To evaluate the options for achieving above considering:
  o Flexibility with carriers
  o Device flexibility
  o Application compatibility
  o Manageability (e.g. ability to control and lock down the devices)
  o Security
  o Integration for existing services, e.g. National Email and Directory Services
  o Cost

• To design and procure a national solution. The procurement of the devices and the cost of the associated airtime and mobile data contracts would remain with the end user organisations.
8. Messaging and Collaboration Services

8.1 Vision

- To provide a rich unified communication service to all users that need it, independent of location. In essence this is providing access to:
  - Telephony services, including voicemail and audio conferencing
  - Email, instant messaging, SMS messages, etc
  - Presence services
- To provide high definition video conferencing systems, desktop video conferencing technologies and other collaboration tools to create a more flexible and efficient working environment.
  - This includes linking to other public sectors and other third parties (e.g. suppliers, patients, etc).
- A minimum number of client applications to be used to deliver the above services in order to optimise the user experience and minimise user training requirements

8.2 Email Services

Current Situation

- A national email service (based on locally deployed servers) is currently being rolled out to NHS Wales organisations. Those that have migrated their users are benefitting from:
  - Support for organisational changes
    - Email address for life (not tied to organisation name)
  - Cost savings as the licenses for the following products have been purchased on a national basis
    - Email anti virus
    - Email archiving
  - Email content monitoring and filtering
  - Accurate, up-to-date address book
  - A minimum acceptable use policy that all organisations have signed up to
- Email services are not provided to all NHS Wales employees. However, with the national email service, these can be provided at no additional cost

Strategic aim

- Implement one national email service for all NHS Wales organisations (and primary care contractors) supported by appropriate third party products and solutions:
  - Provide email mailboxes for all NHS Wales staff. *This will remove the need for third party mailbox services, e.g. doctors.net*
- One common national acceptable use policy
• Migration of mailboxes from locally hosted servers to a nationally hosted email service for all of NHS Wales
• Secure remote access to the national email service from the internet, third party networks (e.g. social services sites) and from approved mobile device (see sections 7.5 and 7.6)
• Establishment of trusted and secure email links to NHSmail and other trusted third party services (police, social services, etc)
• Use of ‘Safe Haven’ mailboxes to facilitate the transmission of person identifiable information using email
• Implement integration of email with a Short Messaging Service (see section 8.7) to allow the transmission of ‘text messages’ via the National Email Service

Proposed next steps
• Migration of all NHS Wales organisations to the national email service
  o Extend the current design for the national email service to accommodate mailboxes for primary care contractors
• Establish trusted and secure email links to NHSmail and other trusted third party services (police, social services, etc)
• Design and implement a solution that allows secure access to email from PCs outside of the NHS Wales network, e.g. from home PCs, or social services PCs
• Design and implement a solution that allows mobile access to email via an approved range of mobile devices
• Creation of a national acceptable use policy for NHS Wales. See the IHC Security Strategy for further information

8.3 Unified Messaging

Unified Messaging (UM) is the integration of different messaging systems (email, voicemail, fax, etc.) into a single ‘message store’, accessible from a variety of different devices.

Current Situation
• Little deployment of UM solutions. Most organisations have voice mail systems available to some users. Some have systems that forward voice mails to users as attachments to emails
• NHS Wales staff are not benefiting from many features of standard collaboration tools that may make their work more effective.

Strategic aim
• A standard UM service deployed across all organisations. This will integrate tightly into the national email service.
Proposed next steps

- Investigate potential UM solutions (telephony system independent products) in the IHC Research Lab
- Recommend a national solution.

8.4 Instant Messaging

Instant Messaging (IM) refers to the functionality that allows users to exchange text based messages over a computer network. Internet hosted IM services include Windows Live Messenger and Yahoo! Messenger.

Current situation

- Ad-Hoc use of internet hosted IM services. Little or no content monitoring or logging is done
- No agreed national standards or hosting strategy may cause local implementations and disparate solutions implemented.

Strategic aim

- Nationally hosted ‘internal’ instant messaging service, with appropriate content monitoring and logging services.

Proposed next steps

- Investigate IM solutions and appropriate third party software in the Informing HealthCare Research Lab
- Recommend a national approach and evaluate options for implementation.

8.5 Presence

Presence systems show a user’s status to other users of the presence system, e.g. available, busy in a call, busy in a meeting, do not disturb, away from office

Current Situation

- Limited or no use of presence systems
- Time and effort is wasted in sending information or requests to staff that are off site or in meetings when a quick response is required and a more suitable recipient may be found.

Strategic aim

- Deployment of a national presence solution which is tightly integrated with the National Email Service
  - Presence users will be able to choose which other users are able to see their status.

Proposed next steps

- Investigate the options for presence solutions. Testing of preferred solution in the IHC Research Lab.
• Recommend a national approach

8.6 Internet Use and Monitoring

This section refers to internet access for the purpose of web browsing.

Current Situation

• Several different content filtering systems used by NHS Wales organisations and the rules applied to these systems differ between organisations

• Local policies exist for internet access. This causes confusion for users that move between organisations. In some cases an action which is acceptable practice in one organisation is a disciplinary offence in another
  o There is no equity in service provision for staff between organisations.

• Some organisations use proxy servers that provide a caching and content filtering/monitoring service. These are purchased on an organisational basis, and as such this does not provide best value for money for NHS Wales

Strategic aim

• One National acceptable use policy for internet access (see the IHC Security Strategy for further information)

• One content filtering solution deployed nationally, and tightly integrated with the national active directory service
  o Management of user accounts and checking of logs, etc would remain an organisation responsibility
  o Caching facilities provided as appropriate to manage the load on the wide area network connections. These would need to be BITS (background intelligent transfer service) compliant

Proposed next steps

• Progress the work in realising the strategic aim. In particular:
  o A national procurement for web content filtering/monitoring and caching service

8.7 Short Message Service

Short Message Service (SMS) is a service for sending short text messages to mobile phones.

Current Situation

• Ad-hoc use of SMS by NHS Wales staff

• Some limited use of SMS in clinical settings e.g. for sending appointment reminders to patients. Feedback indicates that this can significantly reduce non-attendances

• Some clinical and administrative work processes may benefit from managed use of such services.
Strategic aim

- Deployment of a national SMS gateway for NHS Wales, in order to maximise the cost saving potential. This will have several interfaces to allow sending of SMS messages from the National Email Service and custom applications
  - System will need to be capable of billing individual NHS organisations for their usage.

Proposed next steps

- Investigate options for a National SMS service
- Investigate options for procurement and implementation of a National SMS service.

8.8 Video Conferencing

Current Situation

- The Welsh Health Video Service (WHVS) is a well established, fully managed, fully supported Video Conference (VC) service, suitable for use in meetings and in certain Telehealth applications
  - The WHVS has recently been upgraded to support High Definition (HD) VC. However, suitable VC endpoints will need to be procured to make use of this.
  - An IP gateway is in place which allows VC sessions to NHS England
- Initially, the service was implemented with guaranteed bandwidth (using network Quality of Service [QoS]) for the every Video Conferencing devices in order to guarantee image quality
  - The implementation of the QoS ‘rules’ have been relaxed and image quality can no longer be guaranteed. This provides a bigger challenge as the uptake of HD VC increases.

Strategic aim

- Increase WAN bandwidth to ensure that guaranteed bandwidth is available to all VC units. See Section 4.2 for further details
- Establish a high speed link to the academic ‘Welsh Video Network’ (WVN). Currently this is only possible by using an ISDN interconnect and this reduces the image quality
- Higher quality VC sessions using HD VC or tele-presence technologies
- Deployment of desktop based VC solution to support ad-hoc meeting requirements. This will be linked into the fully managed WHVS to allow users on either system to have video conferences with each other
- Strategically placed High Definition or Tele-presence VC suites located around Wales which can be used by all parts of the public sector

Proposed next steps

- Increase WAN bandwidth *(See Section 4.2)*
- Investigate options for connecting the WHVS to the WVN
8.9 Collaboration Tools

This section refers to tools (other than video conferencing) that allow users to collaborate with each other when working in different geographical regions.

Current Situation

- A limited audio conferencing facility is available as part of the WHVS service
- Third party collaboration tools for audio conferencing and data collaboration (desktop sharing, etc) are used on an ad-hoc basis
- Collaboration (other than Video conferencing) is not standardised and can cause unnecessary problems when setting up.
- Collaboration with users outside of the NHS network, using internet hosted collaboration tools such as GotoMeeting or WEBEX, is blocked by most organisations as it is possible to use them to allow unauthorised users to remotely control PCs or potentially share sensitive information.

Strategic aim

- Creation of a new virtual meeting and collaboration solution that can be used by users throughout NHS Wales (and appropriate third parties) without needing specialist Video Conferencing hardware. Ideally, this would be hosted on the PSBA network so that it would facilitate joint working with other public sector organisations.
- A nationally hosted NHS Wales SharePoint site, maximising the benefits from the Microsoft Enterprise Agreement and the using the national active directory for user authentication.

   See also the ‘Strategic aim’ and ‘Proposed Next Steps’ of section 7.5 for additional information around supplier access to NHS Wales resources

Proposed next steps

- Design and implement national SharePoint services for NHS Wales
- Request that PSBA project team investigate options for delivering a virtual meeting and collaboration tools for the public sector in Wales

8.10 Internet facing information services

This section refers to NHS Wales’ websites and other internet based information services.

Current Situation

- NHS Wales' web sites are hosted via a variety of organisations
  - Some through third party, commercial organisations (e.g. Sequence)
  - Some by HSW
  - Some by other NHS Wales organisations
- Different technologies and content management systems are used to deliver the content
• Various third party mailing list services are used for communications with partners and the public

**Strategic aim**

• Consolidated approach to delivering internet information services, hosted centrally by NHS Wales.
  o Highly available services where required.
• Rationalised number of content management systems
• An NHS Wales, or PSBA, hosted mailing list service

**Proposed next steps**

• Review existing contracts with Service Providers
• Design a highly available server farm for hosting internet facing web sites.

### 8.11 Voice services

This section refers to the telephony services that are used in NHS Wales.

**Current situation**

• Since 1989, (the advent of the original Digital All Wales Network which carried voice calls and computer data) a private NHS Wales Wide telephone network has existed. This is known as the Welsh Health Telephone Network (WHTN) and has formed the basis of all telephony within NHS Wales
  o Calls between phone systems connected to the WHTN are toll-free as they are carried ‘On-Net’ (on the network). Significant cost savings have been realised as a result of this.
  o To date, most of the primary care sector have not been connected to the WHTN
  o The WHTN is fully compatible (and connected) to the Government Telephone Network (GTN) and therefore allows on-net calls to any sites connected to the GTN
    ▪ There are no plans to change or remove the GTN interconnect. Instead, it is likely to have a revival with the advent of the PSBA network, because the Welsh Assembly and Local Government are existing users of the GTN. Maintaining NHS Wales’ GTN capability will only serve to promote improved communication, at no charge over the GTN, to these other sectors. It also provides an alternative route, in the event of a problem with the public telephone network
  o In 2002, NHS Wales migrated its Wide Area Network services to dawn2. This is the second generation of the Digital All Wales Network and is an IP only network. At this point, it was planned to migrate the WHTN to a Voice over IP (VoIP) solution so that the telephone calls could be carried on dawn2
    ▪ However, due to technical difficulties (caused by the immaturity of VoIP products at that time), this did not happen. Instead, the WHTN was kept operational by making use of Cable & Wireless’ voice VPN (Virtual Private Network) acting as the core network carrier for the voice traffic. Despite this, the concept of the
WHTN is still in place and toll-free calls are still achieved via the Cable and Wireless service

- Several NHS Wales organisations have implemented IP Telephony (IPT) and Voice over Internet Protocol (VoIP) within their own network. Products from various telephony providers are in use. There has been no national guidance or standards in this area, and as such the implementations vary across Wales

**Strategic aim**

- The concept of the WHTN should continue
  - Toll-free calls between phone systems connected to the WHTN
  - It provides an alternative means of communication in the event of a failure of the Public Switched Telephone Network (PSTN)
  - WHTN to be extended to allow for connectivity for Primary Care sector
  - WHTN (and other inter-PABX trunks) to be migrated to VoIP solutions and carried over the IP network (PSBA network – see section 4.2)
  - National Standards to be set for IP Telephony systems

**Proposed next steps**

- Review the current status of voice services in NHS Wales, with particular focus on the extent of deployment of IP Telephony in local organisations

- Evaluate options to incorporate IPT fully into the national infrastructure, building on the national active directory (see section 9.2) and taking into account the new PSBA core network

  - A full deployment of an IPT-based services will require the development of a consistent numbering regime across NHS Wales and this will impact the existing IP addressing scheme discussed in section 4.6

9.1 Vision

- A National Directory Services that:
  o Allows users to easily identify colleagues in all NHS Wales organisations
  o Allows users to access basic I.T. services from any computer in any organisation
  o Allows users to easily share appropriate information with colleagues in other organisations
  o Allows users to move between organisations
  o Supports organisational reconfiguration.

- A single electronic identity for every NHS Wales staff member
  o Assurance processes in place to ensure that the staff member is who they claim to be when the electronic identity is assigned to them.
  o Appropriate technologies in place to secure the use of the electronic identity (i.e. having a multi factor authentication process, not just relying on username and password combinations)
    ▪ This would also allow for the digital signing of electronic documents

Please see the National Security Strategy for NHS Wales for additional information on user identity management

9.2 User Directory Services

The user directory holds user account details and provides network authentication and authorisation services.

Current Situation

- A national user directory (based on Microsoft Active Directory) is currently being rolled out to NHS Wales’ organisations. Those that have migrated their users are benefitting from:
  o Little or no changes during organisational reconfiguration
  o Easier information sharing and collaboration with other NHS Wales organisations

- For organisations that have not yet migrated
  o Each NHS organisation manages their own user directory service
    ▪ Different products and versions used throughout NHS Wales
  o Accessing services across organisational boundaries is difficult
  o Sharing information across organisational boundaries is difficult
  o Organisational reconfiguration is difficult to deal with

- A self service password reset tool has been procured and is being configured and tested in the IHC Research Labs.
Strategic aim

- All NHS Wales organisations are using the national active directory
- All new applications (across NHS Wales) use the national active directory for authentication.
  - Authorisation using the national active directory will be used, where appropriate
- User account provisioning and de-provisioning process is tightly integrated with appropriate HR systems (e.g. Electronic Staff Record) and other user databases
- Self service password reset tools provided for all users, in order to reduce unnecessary calls to I.T. helpdesks
  - This will also facilitate the mandating of stronger (‘complex’) passwords on the national active directory

Proposed next steps

- Deployment of the self service password reset tool and a move to stronger passwords for authentication
- Development of an Identity Management solution for automatically provisioning and de-provisioning user accounts in the national active directory and mailboxes in the national email service
- Development of tools and/or processes to improve and maintain data quality in the directory

9.3 National Email Directory

This refers to the NHS Wales directory of email addresses, typically accessed via Microsoft Outlook’s ‘Global Address List’.

Current situation

- The national email directory is provided as part of the national email service
  - Those organisations that have not yet migrated to the national email service are not fully benefitting from this
- The quality of the data in the address book needs to be improved

Strategic aim

- All users are using the national email service, where they will received an accurate address book
- Some address book information is automatically synchronised to other ‘authoritative’ sources of information (e.g. ESR). This would be done as part of the user account provisioning tool described in section 9.2
- Users are able to automatically update some of their own information.

Proposed next steps

- Migration of all NHS Wales organisations to the national email service
• Develop or procure a tool which allows users to manage elements of their own entry in the national email directory

9.4 Certificate Services / Public Key Infrastructures

For more information on this section, please see the Security Strategy for NHS Wales.

Current situation

• Ad-hoc use of certificate services within NHS Wales, but no assurance processes in place to accompany these. They are typically used for authentication to wireless networks
• SSL certificates (web server certificates used with HTTPS) are purchased from trusted third parties

Strategic aim

• NHS Wales National PKI supporting
  o Strong authentication
  o Document signing
  o Encryption
• National certificate management solution for NHS Wales
• Nationally approved certificate carrying devices and readers for use throughout NHS Wales
  o This is likely to be a smart card based system

Proposed next steps

• Design and deploy a secure PKI for NHS Wales
• Design and deploy a certificate management services for NHS Wales
• Investigate certificate carrying devices in the IHC Research Lab
# Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>Third Generation Network. A technology that allows data transmission over a mobile phone network. Supports faster data rates than GPRS.</td>
</tr>
<tr>
<td>AirWave</td>
<td>A digital mobile radio service (with a limited data transmission capability) used by the emergency services.</td>
</tr>
<tr>
<td>DAWN</td>
<td>Digital All Wales Network. The legacy multiplexed (telephony and data) Wide Area Network.</td>
</tr>
<tr>
<td>dawn2</td>
<td>The successor to DAWN. dawn2 is an IP-only network, but is capable of carrying voice and video traffic.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Services.</td>
</tr>
<tr>
<td>GBps</td>
<td>Unit of data transmission speed. 1Gbps is 1000 Mbps (bits per second).</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio System. A technology that allows data transmission over a mobile phone network.</td>
</tr>
<tr>
<td>GTN</td>
<td>Government Telephone Network. Pan Government virtual private network developed to create a more cost effective solution for communication.</td>
</tr>
<tr>
<td>IHC</td>
<td>Informing HealthCare. The national IT programme for the NHS in Wales.</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging. Refers to the functionality that allows users to exchange text based messages over a computer network. Internet hosted IM services include Windows Live Messenger and Yahoo! Messenger.</td>
</tr>
<tr>
<td>IP address</td>
<td>An address that uniquely identifies each device connecting to a computer network. An IP address consists of 4 numbers in the format A.B.C.D (e.g. 10.34.232.79)</td>
</tr>
<tr>
<td>IP-SEC VPN</td>
<td>Internet Protocol Security. A suite of protocols used to implement secure exchange of data at the IP layer.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>IPT</td>
<td>Internet Protocol Telephony. Telephony systems that work by using VoIP technology.</td>
</tr>
<tr>
<td>Kbps</td>
<td>Unit of data transmission speed. 1 kbps is 1024 bits per second.</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network. This is the data network physically located within one site e.g. Hospital, Clinic and GP surgery.</td>
</tr>
<tr>
<td>Mbps</td>
<td>Unit of data transmission speed. 1 Mbps is 1000 kbps.</td>
</tr>
<tr>
<td>N3</td>
<td>The New National Network used in NHS England and NHS Scotland (see <a href="http://www.n3.nhs.uk">www.n3.nhs.uk</a> for more details).</td>
</tr>
<tr>
<td>NHSmail</td>
<td>A national email service available to NHS users in NHS England and NHS Scotland.</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet. A technology that allows the transmission of electrical port, in addition to data, over standard twisted-pair cables used in computer networks.</td>
</tr>
<tr>
<td>Presence</td>
<td>Presence systems show a user’s status to other users of the presence system (e.g. available, busy in a call, busy in a meeting, do not disturb, away from office)</td>
</tr>
<tr>
<td>PSBA</td>
<td>Public Sector Broadband Aggregation. A Welsh Assembly Government initaitive to provide a national, pan-sector broadband network.</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service. A technology that allows certain types of data to be given a higher priority than others, when carried on a computer network. Typically used with Voice over IP (VoIP) and IP based Video Conferencing (VC) systems.</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification. A technology for wireless recognition of devices using radio waves. RFID systems used in conjunction with WLANs can support the location tracking of objects.</td>
</tr>
<tr>
<td>Rights Management</td>
<td>Access control technologies used to limit user access to digital information</td>
</tr>
<tr>
<td><strong>SAN</strong></td>
<td><strong>Storage Area Networks</strong> refers to networked storage systems that allow more flexible and efficient use of data storage than traditional storage solutions. SANs typically provide high speed access to large, highly available storage solutions.</td>
</tr>
<tr>
<td><strong>SCCM</strong></td>
<td><strong>System Centre Configuration Manager</strong>. A software package from Microsoft designed to assist with the management of computer systems.</td>
</tr>
<tr>
<td><strong>SMS</strong></td>
<td><strong>Short Message Service</strong>. A service for sending short text messages (up to 160 chars) to mobile phones.</td>
</tr>
<tr>
<td><strong>UM</strong></td>
<td><strong>Unified Messaging</strong>. The integration of different messaging systems (email, voicemail, fax, etc.) into a single 'message store', accessible from a variety of different devices.</td>
</tr>
<tr>
<td><strong>VoIP</strong></td>
<td><strong>Voice over Internet Protocol</strong>. A technology that allows telephony calls to be transported over an IP enabled computer network.</td>
</tr>
<tr>
<td><strong>WAN</strong></td>
<td><strong>Wide Area Network</strong>. This refers to the network links that are used to interconnect NHS Wales’ computer systems on different physical sites.</td>
</tr>
<tr>
<td><strong>WDS</strong></td>
<td><strong>Windows Deployment Services</strong>. A software package from Microsoft designed to assist with deploying operating systems to computers.</td>
</tr>
<tr>
<td><strong>WHTN</strong></td>
<td><strong>Welsh Health Telephone Network</strong>. NHS Wales’ national telephone service.</td>
</tr>
<tr>
<td><strong>WHVN</strong></td>
<td><strong>Welsh Health Video Network</strong>. NHS Wales’ national video conferencing service.</td>
</tr>
<tr>
<td><strong>WLAN</strong></td>
<td><strong>Wireless Local Area Networks</strong>.</td>
</tr>
</tbody>
</table>