General Practice IT Infrastructure Specification

NHS England INFORMATION READER BOX

Directorate		
Medical	Commissioning Operations	**Patients and Information**
Nursing	Trans. & Corp. Ops.	Commissioning Strategy
Finance		

Publications Gateway Reference:	**2221**
Document Purpose	Resources
Document Name	General Practice Infrastructure Specification
Author	NHS England, Strategic Systems and Technology
Publication Date	29 September 2014
Target Audience	• General Practice IT admins • General Practice IT Commissioners (CCGs) • Those supporting the commissioning of General Practice IT • Those involved in the implementation of GP IT, including Systems of Choice, for General Practices such as CSUs and HIS.
Additional Circulation List	
Description	This document defines the core information technology considerations when implementing IT systems for use by GP Practices. It will provide a basis which commissioners can use to define equipment configuration and service levels to support GP Practice IT Operations.
Cross Reference	Securing Excellence in GP IT Services: operating model 2nd edition (2014-16)
Superseded Docs (if applicable)	N/A
Action Required	N/A
Timing / Deadlines (if applicable)	**N/A**
Contact Details for further information	Primary Care IT Team Strategic Systems and Technology Quarry House, 7E24 Leeds LS2 7PD england.digitalprimarycare@nhs.net www.england.nhs.uk/ourwork/tsd/sst/it-pc/

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet

General Practice IT Infrastructure Specification

Version number: 1.0

First published: September 2014

Updated: (only if this is applicable)

Prepared by: NHS England

Contents

1 Introduction

1.1 Purpose of Document

This document defines the core information technology considerations when implementing IT systems for use by GP Practices. It will provide a basis which commissioners can use to define equipment configuration and service levels to support GP Practice IT Operations.

The document outlines decision areas that must be considered to successfully commission and implement IT solutions on which to run and support the GP Practice clinical and operational IT systems.

1.2 Audience

This document should be read by;

- General Practice IT admins
- General Practice IT Commissioners (CCGs)
- Those supporting the commissioning of General Practice IT
- Those involved in the implementation of GP IT, including Systems of Choice, for General Practices such as CSUs and HIS.

1.3 Scope

This document will not cover all equipment used in a GP Practice. This document covers:

- Core Infrastructure; for example networking
- Server Configuration; for example service resilience
- Workstation Configuration; for example processor and memory
- Peripheral Considerations; for example printing
- Additional Considerations; for example additional assessment tools or constraints on device selection

NOTE: This document covers some limited aspects of disaster recovery (DR) and business continuity (BC), but several aspects of DR and BC are now handled by the GPSoC suppliers as part of their remotely hosted solutions. Readers must ensure they are familiar with the relevant aspects of DR and BC in a general practice context, including the content of Securing Excellence in GP IT Services[1] (the GP IT operating model) and the relevant roles and responsibilities as laid out in the CCG Practice agreement.

[1] www.england.nhs.uk/ourwork/tsd/sst/it-pc/

2 Background

Previous documents that have covered GP infrastructure and systems requirements have made prescriptive recommendations. This has led to documents being out of date almost before publication, and to perceived inflexibility in support and solutions.

This document seeks a different approach by offering guidance and a framework that can be used to determine equipment and service capabilities. Those commissioning and implementing GP systems will be guided in determining the operational needs of the practice, translating these to device and service configurations such that appropriate selections can be made.

3 Summary

Asses your business needs, commission services and infrastructure to support them over

a) The expected life time of the service/infrastructure
b) The expected business needs during the infrastructure lifetime

A lot of equipment bought today is expected to last 4 or more years, and the mean IT depreciation cycle employed by NHS England is five years; this could cover the deployment of two major revisions of operating system and or applications.

There could also be paradigm shifts in computing needs; witness the rise in tablet computing since the release of the Apple iPad in the middle of 2010 and the associated move from large static applications to small frequently updated ‘apps’.

As more and more information is available you must take steps to ensure the data is protected. Ensure data is stored securely, by the application and or the device; ensure that the data is transmitted securely, by the application and or the device/network. Take steps to protect infrastructure from un-authorised access; both physically (building security) and remotely (network security.)

While it might be more expensive to build in some expansion room initially, it is usually cheaper than adding to already purchased equipment at a later date.

4 Warranted Environment Specifications

A Warranted Environment Specification (WES) is provided by system vendors and is the environment; architecture, operating system, browser etc., in which their system is supported. Each system in use will generally have its own WES; from the operating system through to office productivity to patient management. While organisations have found that systems will work outside the warranted environment the supplier may not support their software if issues are experienced.

The Spine national service, for example, has its own warranted environment specification. The latest version of that specification and additional details can be found at the following URL;

http://systems.hscic.gov.uk/spine

You should contact the supplier of the systems being purchased for the Warranted Environment Specification for their system. This is true for not only the GP IT systems but Office productivity suites and other systems in use.

Some warranted environment specifications may conflict with others, for example a GP system may require a particular browser version while the Spine may not be supported with that version. There are a number of approaches to solving this,

- working with the suppliers with conflicting specifications to attempt a broadening of warranted environment (preferred)
- using a terminal services type solution (for example Citrix) or Virtual Desktop Infrastructure (VDI) approach
- using a 'Thin App' solution; supports two versions of the same application coexisting on the same machine
- deploying two, or more, machines where conflicts occur
- combinations of the above

Which solution you chose will depend on the needs of the business, the needs of the solution, and the type of conflict.

Guidance

1) When determining the infrastructure solution the WES for national and local applications in use must be consulted.
2) Where specifications conflict attempt resolution with the suppliers before implementing technical solutions.

5 Core Infrastructure

Core Infrastructure covers the equipment and services required to support end user devices and software. Examples of this might be network cabling and internet connectivity.

5.1 N3

The NHS network, N3, is a private network that organisations must connect to in order to enable access to some NHS national systems. It is not, as some think, a secure network. Devices and systems connected to it must still enforce access controls to resources and protect information transferred between applications.

The 'Information Governance Toolkit' assessment process must be completed before an N3 connection is granted[2]. This will mandate some core infrastructure configurations and service provisions; these take precedence over guidance given in

[2] https://nww.igt.hscic.gov.uk/

this document. A ‘Frequently Asked Questions’ about the Toolkit is available at the following web address - http://systems.hscic.gov.uk/infogov/igfaqs/faqigt

Guidance	1) N3 configuration requirements take precedence over any conflicting core infrastructure guidance in this document.

Other services may have additional or even conflicting requirements. In addition the reader should be aware that planning for a successor to N3, the Public Service Network for Health[3], is being investigated and expected to go live in 2015 / 2016. This new network may well have its own, different, requirements which must be considered.

Operational needs and costs must be balanced to determine the correct approach to meeting these needs. For example separate networks, devices or virtualisation may be required.

5.2 Networking

5.2.1 Capacity

The network must have enough capacity to support normal usage and, ideally, with some room for intermittent heavy loads or ‘burst’ traffic.

Capacity is normally measured in the speed or bandwidth of a network connection measured in Mbps. However network capacity can be reduced by latency – delays in processing network data usually introduced at routers and bridges. The greater the latency on a network the slower it will be perceived. Another factor is the number of computers connected to a network, the greater the number and the busier they are the slower the network will be seen.

Measuring usage on a network is not a simple task and usually requires monitoring the network using dedicated tools and software over a period of time. This will give a baseline profile of network usage and an objective indication if capacity is inadequate for the needs. Software vendors may also be able to give indications of network usage by their software.

Quality of Service (QoS) can be used to impose restrictions or to provide preferential delivery service for specific applications or types of network traffic. For example IP telephony or video services might be given preference on a network reducing the capacity for carrying data traffic. If preferential levels of service are required you must ensure that the network has the capacity and the capability to support the required levels. Not all network infrastructures can support all types of QoS control.

[3] http://systems.hscic.gov.uk/centralnetworks/future

Guidance	1) Measure usage to generate a baseline profile and determine if capacity is exceeded 2) Consult vendors for indicative network requirements 3) Determine if QoS is required and any changes this will require on the network capacity and infrastructure capability

5.2.2 Fixed

Over and above the points raised in section 5.2.1 ensure that there are

- enough network ports for the number of devices
- the ports are close to where the devices will be located
- the cabling is of sufficient standard to support the required network speeds Ethernet cables will typically either be Cat 5 supporting speeds of up to 1Gb or Cat 6 supporting speeds of up to 10Gb. Both are limited to lengths of 100m or less between devices. (The maximum speeds are usually only obtainable over cable runs significantly shorter than the maximum run.)
- Cabling is sourced to support the capabilities of current or near term network devices; it is cheaper to install more capable cabling once than to have to replace less capable cabling later.

5.2.3 Wireless

Over and above the points raised in section 5.2.1 ensure that the

- network is secured so only authorised devices can connect. There are many different ways to secure wireless networks. Some protect the data in transit (WEP, WPA, WPA2) by encrypting it while others, MAC Access List, certificate based access controls, etc., stop unknown devices from connecting to the network in the first place. See section 5.4 below for details on existing Good Practice Guides on network security.
- there is coverage where it is required
- there is no coverage where it is not required; the wireless network does not leak outside the building

5.2.4 Mobile

Mobile communications are used by devices such as mobile phones and other devices with SIM card capabilities. Different network types are available. At the time of writing 3G is the most prevalent in England. However the next generation, 4G, is being rolled out and will offer higher connectivity speeds for data. The type of network that can be used for mobile communications is dependent on the device being used and the availability of that network in the area of coverage as well as, to some extent, the service provider.

If mobile network coverage is required organisations should consult with service providers to determine the one that provides the best coverage in the intended areas of usage; which may not be the practice itself if devices will be used by community nurses.

The HSCIC Infrastructure Security Good Practice Guides offer advice on Wireless Security and other topics. See section 5.4, below, for details.

5.2.5 Network Protocols

There are a number of network protocols in use on networks that different services and software packages use to communicate. The most common are TCP and UDP over IP, however others may be used.

Ensure that the network can reliably support the required protocols.

Also look to the future and understand potential near term changes that may impact network provision. For example a standard protocol in use on networks today is TCP/IP v4. However TCP/IP v6 is the next version and addresses some of the shortcomings of TCP/IP v4; including auto-configuration, extensibility, address space (number of devices) and IP security. Not all currently deployed network infrastructures can support TCP/IP v6 and may require upgrading.

Guidance	1) Ensure the commissioned core infrastructure can support the protocols required today 2) Have a road map to implement support for near horizon protocols as required

5.3 Remote Access

Where remote access to resources held on the premises is required steps must be taken to ensure that such access can only be achieved by authorised users. Such access should be carefully audited to ensure breaches are tracked and remediated.

Controls are usually in the form of

- two factor authentication, e.g. using RSA tokens or smartcards
- may also be limited to specific devices e.g. users may not connect from internet café or home machines but only organisation managed devices.
- See section 5.4, below, for details on existing Good Practice Guides on Remote Access security.

5.4 Security

There are many levels of security; this section will look at provision on the core infrastructure, i.e. the network. Other areas, such as workstation security, will be covered in later sections.

The HSCIC Infrastructure Security team have created a number of Good Practice Guides which provide advice in the technology-specific areas of Information Security and Information Governance. The guides cover topics such as Wireless LAN, Fixed LAN, N3 and other areas. The reader should review these documents for additional guidance and requirements.

http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/index_html

Protecting the network usually comprises stopping unauthorised access either by people on the outside trying to get in or by stopping people connecting unauthorised devices to the network on the premises.

Security should enable safe usage rather than block staff from doing their job.

5.4.1 Firewalls/Edge Protection

A good network firewall will protect the internal network from many external threats and help preserve internal network bandwidth. The Firewall Technologies Good Practice Guide provides additional information.[4]

Firewalls can operate at a number of different levels. The most basic is to prevent connections to and from a known list of internet addresses and or by a known list of types of traffic, for example to stop all inbound FTP (File Transfer Protocol) traffic but allow all outbound web / browser traffic.

At a deeper level a firewall can inspect the traffic passing through it, open each packet of network data, to determine if it is malignant for example, and block it if required. This can introduce delays as traffic is inspected but provides a greater level of protection.

It is important to configure the inward facing part of the firewall as well. For example if machines on the internal network should never make FTP connections to external machines, ensure this is blocked. FTP can be used to transfer data to external sites which could result in unauthorised data transfers/leakage.

5.4.2 Unauthorised Connections

There are a number of ways to block unauthorised connections to a network, some more complex, and costly, than others. The more difficult it is to connect an unauthorised device the more management is, usually, required when new devices need authorising.

If all services on the network are configured to talk securely to each other and services are protected by strong authentication protocols the need to prevent unauthorised connections can be reduced.

[4] Firewall Good Practice Guide http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/index_html

Guidance

1) Determine how securely information is protected in transit to determine the effort to expand preventing connections
2) Install a firewall and only allow authorised inbound and outbound traffic
3) Use white listing rather than black listing where ever possible
4) Log network access and audit the logs on a regular basis

5.5 Power

The building must have enough power to support the number of devices that will be run at the same time. In addition it is worth reviewing if, in the case of a power cut, any of the devices should be connected to an Uninterruptable Power Supply (UPS) so they can continue to run during the outage. It should be noted that a UPS is intended to cover short duration power interruptions, max 20 minutes or so (depending on the load). Longer power interruptions would require transition to backup power, for example a generator.

Calculating power requirements is often a case of consulting each device to find out how many Watts it uses and totalling the amount. You may then need to consult with your local electricity provider to determine if the supply to the building is sufficient.

When determining UPS needs you need to ascertain if devices need to run just long enough to be shut down properly or if they need to run for an extended amount of time. The longer a UPS needs to run and the more devices it needs to support the larger and more expensive it will be. UPS needs will also be governed by the business continuity and disaster recovery plans in place.

Guidance

1) Ensure the power supply to the building will support the expected power needs
2) Review UPS needs and only purchase required capacity
3) Consider a generator if power outages are expected to last more than 20 minutes or if the UPS costs exceed those of a generator.

6 Server Configuration

Servers are used in some practices for a number of purposes;

1) Local centralised file storage / backup
2) Document scanning
3) Providing network services, such as DHCP, DNS, Authentication and Directory Services
4) Hosted Application resilience

Where systems are used for Hosted Application resilience the GP IT supplier will generally provide a minimum specification for the system. The specification will often by determined by the number practices to be supported and the number of users.

Review the workstation configuration section for other sizing areas such as disk space and memory size.

6.1 Business Continuity and Disaster Recovery

Where the server is not providing resilience you should ensure that it has been sized to support the services required. If those services are business critical then plans must be in place to ensure that, in the event of failure, the business can continue or, in the worst case, recover within the required time scale from any significant disaster.

This might include

- provision for offsite back up or storage of data
- supply of an identical replacement system within a specified time

Regardless of the mitigation measures taken they should be proportionate to the risk.

Guidance

1) Create, Implement and Test Business Continuity and Disaster Recovery Plans in line with the GP IT operating model and the CCG Practice agreement
2) Ensure the cost of BC and DR plans are proportionate to business need

7 Workstation Configuration

How the workstation is configured has a very large effect on how service provision is judged by users. There are a number of factors, explored below, that must be considered when configuring user workstations. In the past specific criteria were given for workstation capabilities, for example CPU speed. This document moves away from that and places an onus on the commissioning organisation to determine requirements based on vendor supplied figures.

You would normally use the suppliers recommended specifications as a starting point for sizing decisions.

7.1 Bring Your Own Device

“Bring Your Own Device” (BYOD) has become a significant discussion area recently with the rise of capable affordable ‘smart’ phones and tablets. The Good Practice Guides referenced in section 5.4 contain guidance on BYOD management. BYOD devices bring their own concerns around protecting any information stored on them due to the lack of control that can be exercised over the device configuration. A careful appraisal must be made of the ability of the device to protect the data to the required levels before enabling those devices to connect. In some cases it is very difficult to stop devices accessing information, for example NHSmail. In which cases it is important that device users are made aware of the risk and liability they assume. Each organisation must have a published an ‘acceptable terms of use’ policy, which all users must sign before accessing IT resources. This is true for BYOD as well as ‘normal’ infrastructure resources.

7.2 Hardware

The hardware covers the physical properties of the device, not only the amount of memory or disk space but also the form factor.

The core principal for determining hardware capabilities is to consult the vendors of the software that will be running on it and use their recommendations to size the hardware.

In addition you should determine which applications are going to be run at the same time. For example you may need to run an email application, a calendaring application, the GP system and another application concurrently. If so the requirements, certainly for RAM, should be added.

Changes to hardware configurations after purchase can be more costly than purchasing systems with additional capability in the first instance. Where ever possible systems should be purchased to allow for some ‘growth’ in needs. Growth is most often required in the amount of RAM installed, aim for 4GB for a 32bit operating system and at least 4GB in a 64bit operating system. Disk Space and processor speeds are less likely to require growth however if given the option, for minimal price differential, faster processors (or more ‘cores’) are usually better.

7.2.1 Processor

The faster the processor the faster, generally, the system can run loaded applications. The processor recommendation will usually be constrained by the operating system. Subsequent application choice my refine the choice, usually ‘upwards’

Processor cores – processors often have multiple cores allowing for the processing of multiple commands at the same time. So a processor with two fast cores may be slower than one with four cores that run at a slightly slower speed. However not all operating systems and applications can take advantage of multiple cores. Consult with the vendors to determine if solutions being purchased will derive more benefit from multiple cores than faster processors.

Care should be taken that the correct processor architecture is selected for the operating system and applications, i.e. 32bit versus 64bit.

If the device is a mobile device the faster the processor, usually, the less time the battery will last. There is a trade-off to be made of speed against battery life.

7.2.2 Memory

The more memory, RAM, that a system has the more applications/data it can load at the same time. Systems with minimal RAM may spend a large amount of time swapping content on and off hard disks. This significantly reduces the speed of the system.

Determine RAM by adding together the requirements of the systems that will be run concurrently, i.e. the operating system, GP system and office productivity suite.

Adding RAM at a later date can be more expensive than buying a system with extra installed at the time of purchase.

32bit systems are limited in the amount of RAM they can use. Installing more than 4GB in a system with a 32bit operating system is unlikely to result in a return on investment.

7.2.3 Hard disk

The larger the hard disk the more programs that can be installed and the more data that can be held locally.

Many applications are now cloud based and information is held externally to the workstation reducing the need for large hard disks.

When purchasing a hard disk ensure it can support the storage requirements of all the software you expect to install, both initially and in the future, that is over the expected lifetime of the device. You may also need significant amounts of storage for operating system ‘swap’ files depending on the operating system chosen and the amount of RAM installed in the machine.

The speed of the hard disk can play an important part in the performance of the system. The faster the hard disk spins the faster information can be extracted from and written to it. This is usually most noticeable when loading programs or if RAM is constrained and information is being continually swapped out of memory to disk.

Solid state disks offer the best performance although, at the time of writing, with a premium price, smaller capacities and limited availability.

7.2.4 Connectivity

Workstations must be able to connect to external devices, printers etc. and networks to exchange information. The type of connections and their capabilities will be governed by choices of service and software.

For example if a 100Mbps network has been installed selecting a network card that only supports 10Mbps would reduce the benefit of the faster network.

However future capability must be considered, for example if a device can be purchased with USB3.0 built in for a minimal price increase over one with only USB2.0, then careful consideration should be given to the extra value of being able to support the newer standard. Although some external devices purchased today may not themselves support the new standard it can be expected that future purchases will.

Guidance

1) Understand the needs of the applications that will be installed
2) Understand the needs of the peripherals that will be connected
3) Determine the maximum resource use (concurrently running applications/connected devices)
4) Use vendor sizing recommendations, processor speed and cores, RAM, disk size, graphics, connections, etc., to specify purchased hardware with possible room for growth over the lifetime of the hardware.
5) Publish and have all users sign an acceptable terms of use policy for use of IT resources; BYOD as well as provided by the organisation

7.3 Applications

Applications can impose very specific requirements on infrastructure. These vary from only being able to use a very specific peripheral device, to disk space to being able to send specific network protocols over specific network ports requiring firewall configuration changes.

Applications should ensure that any data they store or send is secured. This is over and above any network or device, for example disk encryption, security that has been configured.

In addition applications need to be managed, for example installing new versions or patches. Sometimes these are automated, other times support personnel may need access to machines to carry out the upgrades.

Some applications require specific access levels on the machines they are running on (i.e. local Administrator). This can cause issues for system management if local users are not allowed such levels. Where ever possible applications should be selected that run in the user context and do not need elevated user rights.

Some applications cannot be installed at the same time on the same computer. This might be due to the application itself or to do with ancillary supporting components. For example one application might require Internet Explorer 7 while to access another Internet Explorer 10 might be required. These issues can be overcome by a variety of approaches such as application virtualisation or using machine virtualisation technology. However implementing these solutions can increase the cost of management of the infrastructure.

Guidance	1) Select applications that do not require elevated user rights 2) Applications should store and send any data securely, see the Good Practice Guides. 3) Ensure applications will not interfere with each other 4) Ensure applications do not need specific network configuration changes, especially if these may reduce network security

7.4 Management

The management of workstations will normally be carried out by a 3rd party with expertise in computer and device management. Some external devices may be supported directly by the manufacturer or a specialist support company.

Robust management processes and capabilities can reduce the down time of equipment. They can also ensure that equipment (software) is kept updated and therefore more secure. However, management can be expensive. One option to reduce management costs is to use remote management capabilities, and reporting / monitoring, on deployed systems. Remote management enables a support technician to remotely access the system in question and see the screen and any errors. This can reduce the time to fix and costs as the technician doesn't have to travel to the site. Remote reporting and monitoring enables the collection of metrics about remote systems to a central location. After analysis this can enable emerging problems to be identified and remedied before they cause a loss of service.

Ensure that support contracts are aligned with the business needs and cost if services are unavailable.

For example having a one hour fix agreement for incidents with a low impact (single GP) and a low urgency (5) might not be cost effective. Nor would having an eight hour fix for high impact and urgency incidents. In the former case an eight hour, or longer, response time would be significantly cheaper and more in line with business needs. The systems supplied under the GP Systems of Choice contract will be covered by a Service Level Specification[5] - a service management schedule. However this does not cover the supporting infrastructure.

7.4.1 Mobile

Mobile devices, tablets and phones are in increasing use. It is important that these devices are also properly managed. This management will include not only deploying software and updates but also being able to delete software and data from the devices in the event of their loss.

[5] http://systems.hscic.gov.uk/gpsoc/performance

7.5 Security

There are multiple levels to security, from protecting against staff being tricked into revealing passwords (social engineering) to anti-virus and anti-malware protection. This section only looks at security as applied directly to data protection and not strategies to protect against social engineering.

The core tenant of data security is that data must be secure at rest, when stored on a hard disk or memory stick etc., and when in transit, that is being transmitted from one device to another. This policy was laid out by the, then, NHS Chief Executive, Sir David Nicholson, who stated that there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS.[6]

The HSCIC Infrastructure Security Team has produced a number of Good Practice Guides aimed at data security (http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/index_html) and these should be consulted. Solutions that are sourced to protect data should meet or exceed the recommendations in these documents for securing data at rest or in transit. Where legal constraints are in conflict with the guides the legal imperative takes precedence.

A good management process that can deploy patches and updated anti-virus or malware products is also a key foundation.

Many devices, computers, include local firewalls to prevent unauthorised access to them from the network. If the local network is compromised, either by the introduction of malware or a rogue device connecting, the device firewall can offer additional protection to the device. If present then local firewalls should be used.

7.6 Virtualisation

Virtualisation can be used to support a number of scenarios from running additional operating systems on the same device (machine virtualisation, Hyper-V, VMWare, Virtual Box, etc.) to running mutually incompatible applications on the same machine (application virtualisation, App-V, etc.).

However using virtualisation can increase costs as additional licenses may be required for software or management of environments becomes more complex.

If there is a clear business need for virtualisation it should be used where required.

[6] https://www.igt.hscic.gov.uk/WhatsNewDocuments/Encryption%20Guidance%2031.1.2008.doc
and
http://systems.hscic.gov.uk/infogov/igap

7.7 Backup

Very little data now resides on desktop hard drives. Most data is held on central servers or in ‘the cloud’. However this does not remove the need for ensuring that data is backed up. How and by whom this is done may well have changed.

Ensure that any data you need to preserve is covered by backup agreements with the relevant service providers. Also ensure that any backups are kept securely and for specified lengths of time as required legally or by professional policies.

If data is backed up and stored off site make sure that, in the event of need, it can be restored or retrieved in line with business needs.

In line with current NHS encryption guidance any Personal Confidential Data stored off site must be encrypted.

8 Peripheral Considerations

Some services, for example printing prescriptions, will have specific requirements on peripherals, i.e. printing to a specific resolution on certain weights of paper/card. Peripheral needs and configurations will change over time and may change faster than the workstations or networks they are connected to.

Consult with software and service suppliers to ensure that the correct devices are bought and these can integrate with the software. Ensure that where possible these support proposed technology changes and capabilities or emerging standards. For example contactless smart cards are an emerging technology in the NHS and may require new types of readers. Some bar codes are now 3D as opposed to linear and will require equipment that can read them.

9 Additional Considerations

The list of areas outlined in this document is not exhaustive, each practice will have local variations and needs that may not be covered. For example agreements with local service providers may require additional considerations. These must be factored into infrastructure configurations.

From a wider perspective changes to

- National Programmes
- Information Governance
- Road maps
- Good Practice Guides
- Legal areas – such as the Data Protection Act
- Professional Guidelines issued by Royal Collages and other professional bodies

will all impact on commissioning decisions for infrastructure and system implementation and support.

9.1 Infrastructure Maturity

Increasing the maturity of your infrastructure and service provision, moving from one of manual configurations to managed systems with automation and pro-active monitoring of services, can result in reduced overall costs and more stable service provision.

The NHS has the "NHS Infrastructure Maturity Model" (NIMM) which organisations can use to assess the maturity of different components of the business and IT. The assessment will give an indication of how mature the organisation is in a particular area and what steps should be taken to improve maturity.

Organisations are encouraged to run the 12 NIMM core capability assessments in the first instance. Once this has been completed, and a road map put in place to improve maturity, assessments that are more specific to each organisation should be selected and completed; the results from these are then incorporated into the road map.

The assessments can be run internally and there is no requirement to report results.

The NIMM can be accessed from www.pspg.nhs.net. Currently an NHS Mail account is required to register for access.

10 Consolidated Guidance Notes

Below is a list of all the guidance points made throughout the document.

1) When determining the infrastructure solution the WES for national and local applications in use must be consulted.
2) Where specifications conflict attempt resolution with the suppliers before implementing technical solutions.
3) N3 configuration requirements take precedence over any conflicting core infrastructure guidance in this document.
4) Measure usage to generate a baseline profile and determine if capacity is exceeded
5) Consult vendors for indicative network requirements
6) Determine if QoS is required and any changes this will require on the network capacity and infrastructure capability
7) Ensure the commissioned core infrastructure can support the protocols required today
8) Have a road map to implement support for near horizon protocols as required
9) Determine how securely information is protected in transit to determine the effort to expand preventing connections.
10) Install a firewall and only allow authorised inbound and outbound traffic
11) Use white listing rather than black listing where ever possible.
12) Log network access and audit the logs on a regular basis
13) Ensure the power supply to the building will support the expected power needs
14) Review UPS needs and only purchase required capacity
15) Consider a generator if power outages are expected to last more than 20 minutes or if the UPS costs exceed those of a generator.
16) Create, Implement and Test Business Continuity and Disaster Recovery Plans
17) Ensure the cost of BC and DR plans are proportionate to business need
18) Understand the needs of the applications that will be installed
19) Understand the needs of the peripherals that will be connected
20) Determine the maximum resource use (concurrently running applications/connected devices)
21) Use vendor sizing recommendations, processor speed and cores, RAM, disk size, graphics, connections, etc., to specify purchased hardware with possible room for growth over the lifetime of the hardware.
22) Publish and have all users sign an acceptable terms of use policy for use of IT resources; BYOD as well as provided by the organisation
23) Select applications that do not require elevated user rights
24) Applications should store and send any data securely, see the Good Practice Guides.
25) Ensure applications will not interfere with each other
26) Ensure applications do not need specific network configuration changes, especially if these may reduce network security