Simple Guide for Hosted Computing in the NHS

Innovation and safety

ETHOS

Simple Guide for Hosted Computing in the NHS

Many NHS organisations are already successfully using hosted services with no recorded increase in risk to patients. The law on outsourcing data is very clear. Data owners are responsible for keeping data safe, in this case to protect patients. This guide aims to run through some of the basic concepts relating to this.

The term 'Hosted Computing Services' includes those commonly referred to as "Cloud Services". The use of "Cloud Computing" or "Cloud Services" has been avoided in this guide to reduce any confusion regarding a solution being 'cloud' or not. Hosted Computing includes 'cloud' offerings.

A growing number of provider organisations are seeking to move their use of computing resources, seeking to take advantage of benefits such as:

- Reduced costs
- Different charging models
- Agile implementation

Uptake within the NHS has been slow to date. By processing data off premise, organisations may have to grapple with hazards and failure modes they have not previously been exposed to with their current operating model.

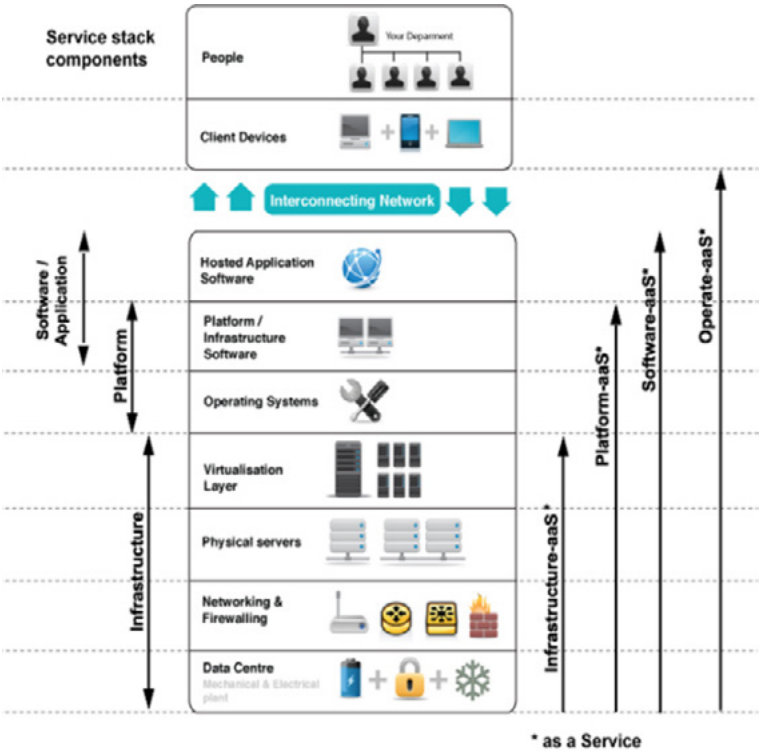
What is Hosted Computing?

Hosted Computing is a term that is used by many people to mean different things and cover a wide range of technologies and operating models. Meaning may also depend on the context. It is therefore important to ensure the reader is clear about our use of "hosted computing" here.

Hosted Computing = On demand access to, usually, off-premise computing via a network.

The definition given is broad and covers a number of these service models.

The model here shows the range of these types of services. Each has its own risk profile and cost.



ETHOS

The lower down the diagram the more risk that NHS organisation may carry. For example, purchasing Infrastructure as a Service (IaaS) carries more risk for the organisation buying it as they must install and manage the operating systems and applications running on top. The hosted service provider is responsible for the physical components and connectivity.

If buying Software as a Service (SaaS) the hosting service provider must operate all layers of the service. This carries greater risk for them and less for the purchasing organisation.

There are also **four** types of deployment models:

1. **Private Hosting** - the customer is the only user of the service. Access to this service is usually restricted to just the organisation buying it.
2. **Community Hosting** - a group of NHS organisations may access resources from the same hosted service provider. Such groups are usually formed where they share specific requirements, such as very high availability needs. This may be too expensive for one organisation to commission. Access to the service will be restricted to the community of organisations who have purchased it.
3. **Public Hosting** - the service is managed by the hosted service provider and made available to the public. Anyone can purchase and use this service and access is, usually, via the internet.
4. **Hybrid Hosting** - this is a combination of one or more of the previous models. Data and applications may be distributed across different types, depending on risk and to maximise value of each service.

What about the Potential Challenges and Benefits?

Hosted Computing services are seen by many NHS organisations as useful in addressing several challenges. Some of these are explored below.

Challenges:

- IT is not a core NHS business to maintain large computer resources in facilities that were not intended for that purpose, but some NHS organisations do just that
- Resource constraints can reduce the ability to innovate and adopt new technology or solutions as they are made available
- Economies of scale cannot be easily realised
- It can be difficult to accurately determine the cost of these systems in the NHS, as power and other facility costs can be difficult to separate from other operating costs. This can also mean that measuring any benefits they deliver can be very difficult to show

Benefits:

- Releasing NHS resources from daily maintenance to focus on adding value to services
- Hosting providers have specialist, skilled IT staff who can manage services across many customers reducing some maintenance costs by providing economies of scale
- Large scale hosting providers can invest to provide a large scale and higher quality service

- Increased utilisation and at scale deployment results in lower cost base of resources which are passed onto purchasing organisations
- Moving expenditure from one-off capital spend to operational expenditure can delivery regular technical refreshes of purchased solutions for no additional outlay and simpler forecast expenditure relating to contracts
- More options for targeting resiliency and system redundancy where/when required
- Payment models move towards ‘pay as you go’

Adoption Blockers and Drawbacks:

- Uncertainty over regulations governing where NHS data can be stored
- Lack of experience in contracting hosted services could lead to increased costs
- Loss of control of the service; perceived or actual
- Fears of interruption of access to the service. This could be because of physical systems/network links are interrupted; business/operational issues; hosted service provider company fails complex supplier demands.
- Fears that organisations may be locked into particular service offerings due to the difficulties and cost of moving the data and services to a new provider

It is worth noting that the telecommunications risks may exist for any off-site system. Uncertainty regarding data being properly segregated from other service tenants could lead to potential data leakage.

This guide does not advocate the transfer of risk away from the NHS organisation. Therefore, organisations seeking to commission a Hosted Computing service must undertake a local hazard and risk assessment in their own operational context.

This **operational context** might include, but are not limited to:

- The service model used: Infrastructure as a Service (IaaS)
- The deployment model: private, community etc.
- The type of information being held: is it personal data/sensitive personal data as defined in the Data Protection Act?
- The location of information that will be held physically and geographically
- The contract entered into for the service, especially provisions which may impact on clinical safety concerns: loss of availability of the service which may lead to delays in delivering the correct care and otherwise avoidable clinical risk to patients

The Greatest Hazard to Patient Care?

Interruption of access to information which can lead to a delay in delivery of appropriate treatment is the greatest potential risk when using Hosted Computing. While this risk is not unique to Hosted Computing new failure methods are introduced into the organisation that need robust evaluation.

A summary of the key recommendations for the use of Hosted Computing in the NHS is given below, split into four main areas:

1. **Physical** - Because information and services are now remote from the point of use, there is an increased risk that the connection linking the NHS organisation and the service provider may be broken. For example by engineering works. Interruption of the connection will lead to loss of access to the data. This risk can be mitigated by service design. For example more than one link using different routes (often known as 'diverse routing'), and contract clauses regarding the service level agreements.

2. **Protection / Security** - There is an increased risk that NHS organisations could breach regulatory requirements and Information Governance guidance through the use of hosted services. This occurs where data is stored or accessed insecurely or in inappropriate offshore locations. These breaches could give access to patient information to those with no legitimate interest and could result in that information being used to harm the patient. These risks can be mitigated by an understanding of the regulatory requirements, clear areas of responsibility backed up by contracts and regular review / auditing.

3. **Regulation** - While guidance in this area is improving those organisations that are leading the way for the rest of the NHS may find themselves exposed to increased risk of inadvertently breaching regulations. Organisations should seek expert assistance in reviewing the impact of regulations on proposed solutions and pursue the "as low as reasonably practicable" approach to reducing risk.

4. **Contract** - Due to the lack of experience using Hosted Services in the NHS, there is a possibility that contracts will not protect patient safety due to inadequate guarantees about access to patient information or restoring access within a timely manner should be interrupted. Organisations should seek expert assistance in drawing contracts and where possible leverage existing industry best practice and experiences from others in the NHS who have purchased systems in the past. The Gcloud procurement portal may offer some assistance:

   gcloud.civilservice.gov.uk/

For more information about ETHOS safety and innovation work please find us on:

@LtdETHOS

linkedin.com/company/ethos-ltd

or email us at: info@ethos.co.im