

**Information Security Policy
Cloud Computing**

Author:	Information Security Manager
Responsible Lead Executive Director:	Director of Information and Digital Technology
Endorsing Body:	Healthcare Quality Assurance and Improvement Committee
Governance or Assurance Committee	Information Governance and Cyber Assurance Committee
Implementation Date:	February 2019
Version Number:	1.2
Last Review Date:	Nov 2023
Review Date:	Nov 2026

Information Security Policy – Cloud Computing

CONTENTS

- i) Consultation and Distribution Record
 - ii) Change Record
1. INTRODUCTION
 2. AIM, PURPOSE AND OUTCOMES
 3. SCOPE
 - 3.1 Who is the Policy Intended to Benefit or Affect
 - 3.2 Who are the Stakeholders
 - 3.3 Scope of Guidance
 4. PRINCIPAL CONTENT
 - 4.1 How to Make Use of Cloud Services in NHS Lanarkshire
 5. ROLES AND RESPONSIBILITIES
 6. RESOURCE IMPLICATIONS
 7. COMMUNICATION PLAN
 8. QUALITY IMPROVEMENT – MONITORING AND REVIEW
 9. EQUALITY AND DIVERSITY IMPACT ASSESSMENT
 10. SUMMARY OF POLICY / FAQs
 11. APPENDIX 1 – REFERENCES
 12. APPENDIX 2 – CLOUD COMPUTING
 - 12.1 What is Cloud Computing
 - 12.2 Drivers and Benefits of Cloud Computing
 - 12.3 Concerns and Challenges Regarding the Use of Cloud Computing
 13. APPENDIX 3 – NHS DIGITAL GUIDANCE ON THE USE OF CLOUD SERVICES

Information Security Policy – Cloud Computing

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	<ul style="list-style-type: none"> Alan Ashforth, Information Security Manager
Consultation Process / Stakeholders:	<ul style="list-style-type: none"> Donald Wilson, Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) Information Governance and Cyber Assurance Committee
Distribution:	<ul style="list-style-type: none"> All staff

CHANGE RECORD			
Date	Author	Change	Version No.
Sept 2018	A Ashforth	<p>First draft : New policy identified and reviewed in line with General Data Protection Regulation (GDPR) and reference to Data Protection Act 2018</p> <p>Second draft: Updates after comments provided.</p> <p>Third draft: More references added</p> <p>Fourth draft: Create an appendix 2 for background on cloud computing</p> <p>Fifth draft: Restructured principle content</p> <p>Sixth draft: Added cloud GPG spread sheet for cloud provider to complete</p> <p>Seventh draft: Altered cloud GPG spread sheet – adding review column</p> <p>Eighth draft: Reinforced need to follow based on legal requirements in view of current data protection legislation</p> <p>Ninth draft: Amended references – hyperlink for one reference needed updated</p>	0.8
Feb 2019	A Ashforth	First issue of policy	1.0
June 2021	A Ashforth	Scheduled review including updated UK GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section	1.1
Nov 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. References Appendix 1 – updated. Broken links to NHS Digital content updated.	1.2

Information Security Policy – Cloud Computing

1. Introduction

This policy relates to cloud computing and forms part of the overall Information Security policy for NHS Lanarkshire.

The use of cloud services in NHS Lanarkshire can provide significant benefits and support the organisation to be more agile in the way it works. However, there are a number of challenges and risks that must be considered and managed. This is particularly relevant when using cloud services to store and process sensitive or confidential information. Most cloud services are not acceptable information transfer mechanisms for Person Identifiable Information (PII) or any other sensitive data, under current data protection legislation.

The recommendation is that the use of cloud services should be encouraged alongside traditional software and infrastructure deployment models providing that the following key principles can be met:

- Value for money and financial fit
- Legal/mandatory requirements can be satisfied, including
 - The General Data Protection Regulation (GDPR) legislation
 - Data Protection Act 2018
 - The Directive on Security of Network and Information Systems (NIS Directive)
- Use of appropriate contractual and technical controls
- Public perception / concerns can be managed
- Supplier tie-in can be managed (exit conditions)
- Appropriate backup, recovery and resilience

It is recommended that the assessment of whether the use of Cloud services is appropriate be undertaken as part of the business case process, prior to any procurement commencing.

This policy details the supplementary security requirements for formal approval using the Data Protection Impact Assessment (DPIA) approval process. This is to ensure a consistent adoption across NHS Lanarkshire and meet the legal requirements as part of the current data protection legislation.

This guidance document provides the context for the use of cloud services by NHS Lanarkshire and outlines the framework which must be followed to ensure that the associated risks have been properly assessed and recorded as part of the business case and DPIA.

This guidance also sets out the approval process which should be followed by all NHS Lanarkshire staff who wish to use cloud services.

2. Aim, Purpose and Outcomes

To ensure that INFORMATION SECURITY is maintained

Information Security Policy – Cloud Computing

- Ensure that confidentiality and integrity of personal and sensitive information is maintained
- Ensure that information is available to **authorised** users
- Ensure that information is not disclosed to **unauthorised** people
- To prevent **destruction** of information

This document forms the NHS Lanarkshire Cloud Computing Policy, in support of the NHS Lanarkshire Information Security Policy. This document is part of the Information Security Management System (ISMS) for NHS Lanarkshire and describes the measures the organisation takes to risk access and manage the use of cloud computing.

Compliance with it will help protect NHS Lanarkshire from disruption and business impact and to protect the data hosted on the cloud platform.

This policy forms part of the Information Security Management System (ISMS) and should be read in conjunction with all the IS policies.

This policy has been written in line with the best practice for information security standards ISO 27001 and ISO 27002 and the policy will be reviewed to meet future changes to this standard.

This policy has been written to comply with current legislation and the policy will be updated appropriately to suit new and/or modified legislation. The references appendix will be updated to reflect this legislation.

3. Scope

3.1 Who is the Policy intended to Affect?

This policy is intended for all NHS Lanarkshire staff to maintain information security. In the interests of clarity all references to 'staff' includes all staff within NHS Lanarkshire and all staff who are employed, engaged or partners within each GP practice (contracted to NHS Lanarkshire).

3.2 Who are the Stakeholders

All staff

NHS Lanarkshire take care to ensure your personal information is only accessible to authorised people. Our staff have a legal and contractual duty to keep personal health information secure, and confidential. In order to find out more about current data protection legislation and how we process your information, please visit the Data Protection Notice on our website at www.nhslanarkshire.scot.nhs.uk or ask a member of staff for a copy of our Data Protection Notice.

Information Security Policy – Cloud Computing

3.3 Scope of Guidance

There are several cloud services deployment methods currently in existence; these are defined later in this document. It should be noted however, that this is a rapidly emerging technology and subject to frequent changes, as such new offerings are regularly brought to the market.

The scope of this policy therefore applies to all hosting models (as defined in Cloud Computing – Appendix 2).

For each hosting proposal, an assessment should be conducted to determine if the criteria are fulfilled. The output of this assessment should be documented and retained for future reference in conjunction with the Data Protection Impact Assessment (DPIA).

The guidance is intended to be followed for all projects considering a move of data to a cloud service.

In the case of existing services already making use of Cloud, it is recommended that the risk assessment be undertaken so that the risk level is known and that the appropriate controls are applied.

For services already under contract with a third party provider, it is possible that action required as a result of this assessment can only be considered at contract renewal.

4. Principal Content

4.1. How to Make Use of Cloud Services in NHS Lanarkshire

It has been agreed that NHS Lanarkshire will make use of the guidance produced by NHS Digital (in conjunction with the Department for Health), within the context of the Data Protection Impact Assessment (DPIA) approval process. This will ensure that a holistic view of the risk is taken and that a consistent view across NHS Lanarkshire is maintained.

When considering whether to make use of cloud services within NHS Lanarkshire, staff must follow the four steps given below, which are based on the [NHS Digital: NHS and social care data: off-shoring and the use of public cloud services](#).

NHS Digital have refined the 14 Cloud Security Principles developed by the National Cyber Security Centre (NCSC) which describes the goals and technical implementation, using a clearly defined risk profile class based on the sensitivity of the data to be hosted, scale/volume, and persistence of the data.

A summary of the main documents that form the NHS Digital advice on cloud security are contained within 'Appendix 3 - NHS Digital Guidance on the Use of Cloud Services'.

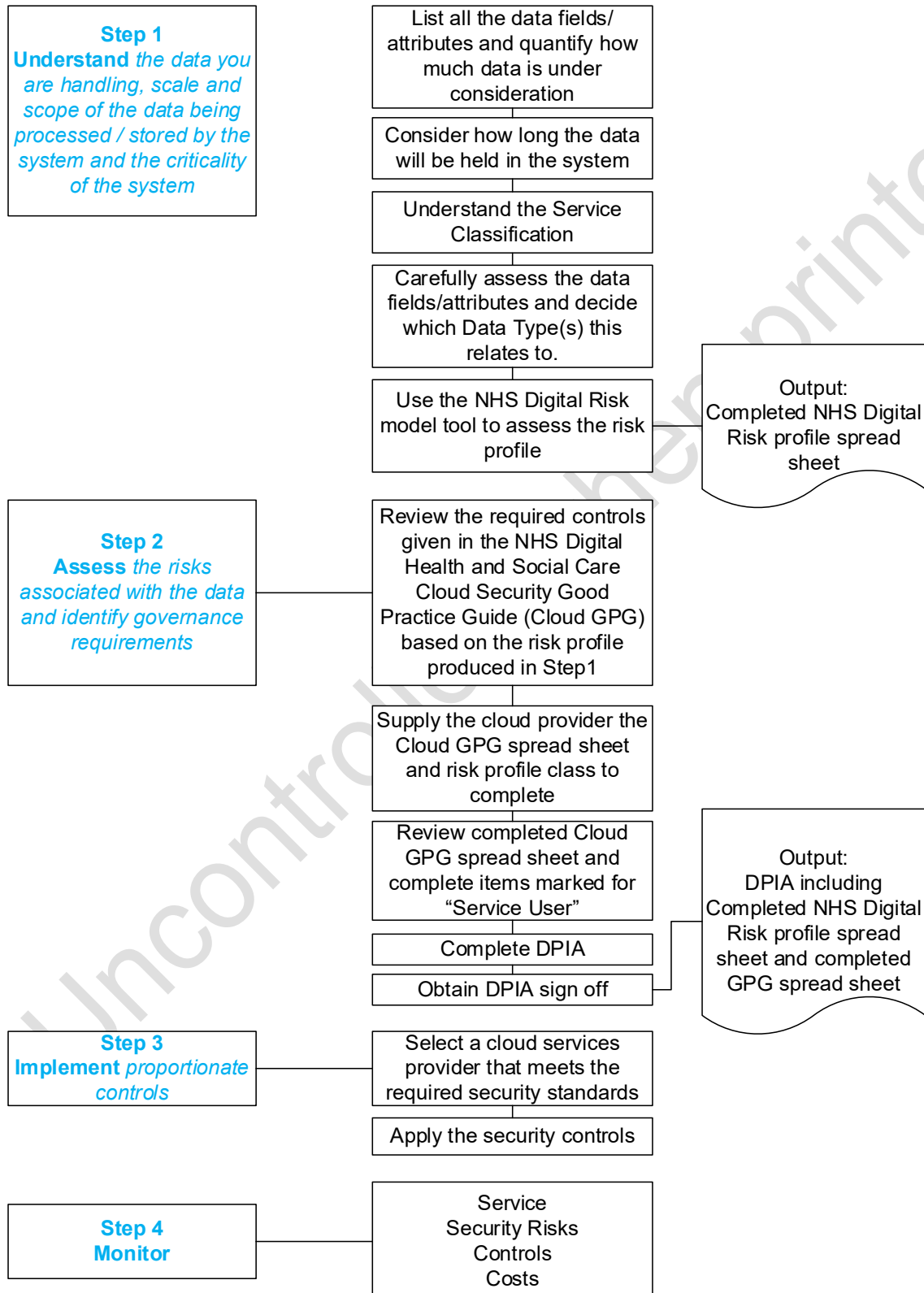
These four steps are in addition to completion of a DPIA and will provide detail on organisational and technical control questions within the DPIA (Q11 and Q12). This is

Information Security Policy – Cloud Computing

mandatory requirement for completion of a DPIA for a cloud based service. The output documents from this process such as the risk assessment and evidence of supplier controls must be inserted into the DPIA.

An overview of the process is as follows:-

How to Make Use of Cloud Services in NHS Lanarkshire



Information Security Policy – Cloud Computing

The complete process is described as follows:

Step 1 – Understand *the data you are handling*:

Understand the scale and scope of the data being processed / stored by the system and the criticality of the system. This should be carried out as part of the business case process, prior to any procurement commencing:

- List all the data fields/attributes that will be stored or processed by the system.
- Quantify how much data is under consideration.
- Consider how long the data will be held in the system.
- Understand the Service Classification (refer to appendix B in NHS Digital [Health and Social Care Cloud Security- Good Practice Guide](#)) of the system (Bronze | Silver | Gold | Platinum). This relates to the availability SLAs and will be used to determine the cloud security approach for availability and integrity. The service classification is normally agreed between the owning Programme and Service management.
- Carefully assess the data fields/attributes and decide which Data Type(s) this relates to, see [Health and Social Care Cloud Risk Framework](#). This framework document lists the different Data Types, scale and persistency along with descriptions and examples.
- Use the NHS Digital [Health and Social Care Data Risk model](#) to profile the risk. When using the risk profile model it is important the definition of a record is carefully considered in order to determine the correct 'scale'. Reference to the guidance notes should be made to ensure this is understood and answered correctly. It must also be remembered that the scale of data will grow over the lifetime of the project - an estimate of the anticipated growth is required and suitable review points should be identified and scheduled.
- The NHS Digital [Health and Social Care Data Risk model](#) calculates a score based on the type of data, the amount of data and for how long the data is held. This score is then translated into a Risk Profile Classification and will be used in the next steps of the process.
- The risk profile classification is used to help you understand:
 - The risk profile and the associated governance that we would expect you to undertake.
 - The controls that are needed to be put in place to mitigate the risk.
- The output of the risk profile model spread sheet should be retained along with the project documentation set. This will be required as part of any future consistency checking that might be required and should also be used during the contract management phase of the agreement.
 - Retain the list of data types/attributes.

Information Security Policy – Cloud Computing

- Record the rationale for selecting the data type(s).
 - Retain the completed risk model.
- The completed risk profile model spread sheet should be an embedded within the DPIA at the end of Q12.

However, proportionate controls are available to help mitigate these risks, regardless of whether the risk is classified as Class I or Class V. These are detailed in appendix A of NHS Digital [Health and Social Care Cloud Security- Good Practice Guide](#).

Step 2 – Assess the risks associated with the data:

Assess the risk and identify governance requirements when utilising cloud services:

- Each request to use cloud services must undergo scrutiny to ensure that it aligns with the [Scottish Public Sector Cloud Computing Guidance 2015](#)
- The risk profile level from Step 1 will help determine the level of project governance required. Different programmes will have different appetites towards risk and this appetite may vary over time.
 - Class I defines the lowest level of risk.
 - Class V defines the highest level of risk.

Using the Risk Profile Classification, refer to the table below to understand the governance expectation.

Risk Profile Classification Level	Expectation
Class I	All organisations are expected to be comfortable operating services at this level.
Class II	Whilst there may be some concerns over public perception and lock-in, most organisations are expected to be comfortable operating services at this level.
Class III	At this level, risks associated with impact of breach become more significant, and the use of services at this level therefore requires specific risk management across all risk classes.
Class IV	At this level, it may become more difficult to justify that the benefits of the using public cloud outweigh the risks. However, a case may still be made, requiring wider approval by NHS Lanarkshire Information Governance Committee. Specialist advice and guidance should be sought.
Class V	Operating services at this level would require board-level organisational commitment, following specialist advice and guidance.

- The risk profile level will clarify where data can reside. While there are no restrictions on where in the UK data may reside there will be restriction on data being stored outside the EEA or countries deemed by the European Commission to have adequate protections for the rights of data subjects.

Information Security Policy – Cloud Computing

- Supply the cloud provider with a copy of the NHS Digital Health and Social Care Cloud Security Good Practice Guide spread sheet (based on NHS Digital [Health and Social Care Cloud Security- Good Practice Guide](#), see Appendix 3), along with the identified risk profile produced in Step 1. The supplier needs use this spread sheet to provide details of the technical controls to meet these requirements.
- Some items on the NHS Digital Health and Social Care Cloud Security Good Practice Guide spread sheet need completed by the 'Service User', this would normally be a member of the Digital Department such as the application manager assigned to the project.
- Complete the Data Protection Impact Assessment (DPIA) with particular attention to the organisational and technical control questions (Q11 and Q12). The completed NHS Digital Health and Social Care Cloud Security Good Practice Guide spread sheet should be embedded within the DPIA at the end of Q12.
- **For requests where the risk profile has been classified as IV or V, it is recommended additional consultation will be required as follows:**
 - **Information Governance Manager (IGM) / Data Protection Officer (DPO) should raise with peers at national Information Governance Forum and with the IG leads for NHSS and Scottish Government Digital Health and Care Directorate**
 - **Should residual risks exist the IGM/DPO may consider whether these residual risks need prior consultation with the ICO.**
 - **Information Security Manager (ISM) should raise with peers at national Information Security Forum and with the IS leads for NHSS and Scottish Government Digital Health and Care Directorate**
 - **IGM/DPO and ISM should raise with NHS Lanarkshire Information Governance Committee and provide feedback from above national groups**
- Obtain formal sign off/approval of the DPIA by:
 - Information Governance Manager (IGM) / Data Protection Officer (DPO)
 - Information Security Manager (ISM)
- Should residual risks exist the IGM/DPO may consider whether these residual risks need prior consultation with the ICO.
- Obtain formal sign off/approval of the DPIA by:
 - Senior Information Risk Owner (SIRO)
 - Caldicott Guardian
- Finally the Information Asset Owner(s) (IAO(s)) may sign off the DPIA, but only after the DPIA has already been approved by the SIRO and Caldicott Guardian.

Step 3 – Implement *proportionate controls*:

Once approval has been given to utilise a cloud solution:

- Select a cloud services provider that meets the required security standards, and

Information Security Policy – Cloud Computing

- Apply the security controls as detailed in the completed NHS Digital Health and Social Care Cloud Security Good Practice Guide spread sheet produced in Step 2.

Step 4 – Monitor:

Once implemented you must continue to proactively monitor and manage the:

- Service;
- Security risks,
- Controls; and
- Costs.

This should be conducted as part of the risk management process, including contract management.

5. Roles and Responsibilities

Authors/Contributors:	Information Security Manager (ISM) Information Governance Manager (IGM) / Data Protection Officer (DPO) Head of Digital Governance
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance and Cyber Assurance Committee

6. Resource Implications

No resource implications

7. Communication Plan

This policy will be managed through the Corporate Policies intranet site and will be announced through the staff briefing.

8. Quality Improvement – Monitoring and Review

To be reviewed at regular intervals by Information Security Manager.

9. Equality and Diversity Impact Assessment

This policy meets NHS Lanarkshire's EDIA



(tick box)

10. Summary of Frequently Asked Questions (FAQs)

N/A

Information Security Policy – Cloud Computing

11. [Appendix 1 - References](#)

The principal Acts of Parliament, Scottish Government circulars, and internal guidance documents relevant to this policy are:

- [Government Cloud First policy](#)
- [Scottish Public Sector Cloud Computing Guidance 2015](#)
- [Scotland's Digital Health and Care Strategy](#)
- [NHS Digital - NHS and Social Care Data: Off-Shoring and the Use of Public Cloud Services](#)
- [National Cyber Security Centre - Guidance - Implementing the Cloud Security Principles](#)
- [UK General Data Protection Regulation \(GDPR\)](#)
- [Network and Information Systems Regulations 2018 \(NIS Regulations\)](#)
- [National Cyber Security Centre Cyber Assurance Framework](#)
- [Scottish Government Public Sector Cyber Resilience Framework](#)
- [CEL 25 \(2012\) NHS Scotland Mobile Data Protection Standard](#)
- [Civil Contingencies Act 2004](#)
- [Computer Misuse Act 1990](#)
- [Copyright, Design and Patents Act 1988](#)
- [Data Protection Act 2018](#)
- [Freedom of Information \(Scotland\) Act 2002](#)
- [MEL 2000 \(17\) Data Protection Act 1998](#)
- [NHSL Risk Management Framework](#)
- [Public Records \(Scotland\) Act 2011](#)
- [Regulation of Investigatory Powers \(Scotland\) Act 2000](#)
- [Scottish Government Records Management: NHS Code Of Practice \(Scotland\) Version 2.1 January 2012](#)
- [SG DL \(2015\) 17 Information Governance and Security Improvement Measures 2015-2017 \(NHSS Information Security Policy Framework\)](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)

Information Security Policy – Cloud Computing

12. [Appendix 2 - Cloud Computing](#)

12.1 What is Cloud Computing

The majority of NHS Lanarkshire's infrastructure and systems are hosted /make use of on-premise computing, whereby all storage and processing resources are held on servers located in health board computer rooms.

Over the last few years there has been a shift in the IT industry to the use of 'Cloud Computing'. The National Institute of Standards and Technology (NIST) defines cloud computing as 'a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'. The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service.

The UK government define the primary characteristic of cloud computing as being an on-demand, self-service model, where consumers of cloud computing should be able to provision computing capabilities, like server time and network storage, as needed without requiring human interaction with each service provider.

In line with the NIST definition, there are three different service models for cloud computing:

- **Software as a Service (SaaS)**. With this model, the service provider delivers a complete software service, including the underpinning infrastructure required to host it. Access to the service is typically via a web browser (*Internet Explorer, Edge, Chrome, Safari, Firefox, etc*).

Examples of SaaS are Microsoft Office 365, Mailchimp, Slack, Trello, Basecamp, Confluence, Stride, Jira Software, Smartsheet, Yammer, Zendesk & GitHub.com and on-line questionnaires - SurveyMonkey, Webropol, SmartSurvey & SurveyApp, and personal storage - Microsoft OneDrive, Google Drive, Dropbox & iCloud.

- **Platform as a Service (PaaS)**. With this model, the service provider delivers a complete platform onto which customers can install and run their own application(s). This allows customers to focus on the delivery of their systems without consideration of the underlying platform.

Examples of PaaS are AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos.

- **Infrastructure as a Service (IaaS)**. With this model, the server resources (processing, storage, backup, etc) are provided by a cloud computing provider to the customer. The customer then installs their own software onto this infrastructure (*e.g. web server, file server, etc*).

Examples of IaaS are Amazon AWS, Microsoft Azure, Rackspace Open Cloud, Google Compute Engine, HP Enterprise Converged Infrastructure, IBM SmartCloud Enterprise, CloudStack, Linode, OpenStack, Cisco Cloud Infrastructure Solutions.

Information Security Policy – Cloud Computing

It should be noted that some cloud computing solutions can exist in more than one service model e.g. Microsoft Azure can be PaaS or IaaS or both.

NCSC suggest a Cloud first approach by using:

SaaS where you can
...followed by PaaS
..and then IaaS

NIST also list four deployment models for cloud computing:

- **Public cloud** – The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of these. It exists on the premises of the cloud services provider.
- **Private cloud** - The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g. business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of these, and it may exist on or off premises.
- **Community cloud** – The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Hybrid cloud** – The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology which enables data and application portability (e.g. cloud bursting for load balancing between clouds).

12.2 Drivers and Benefits of Cloud Computing

There are many features which make the use of cloud computing by NHS Lanarkshire attractive.

These include:

- **Fast to provision** - typically, cloud services can be signed-up to and paid for easily, with the service being available for immediate use (or with a very short lead-time). This assumes that no design and configuration work is needed; however this is not usually the case.
- **Specialist resource** - less specialised IT skills are needed by the customer to deploy and manage a cloud delivered service as the majority of the resources required are supplied by the cloud provider. This can be an advantage where recruiting and retaining staff with specialised IT skills is difficult.

Information Security Policy – Cloud Computing

- **Pay as you use** – rather than paying a fixed amount per day/week/month, cloud services are typically billed for in line with what is actually consumed. This can result in lower costs being paid but can also be difficult to budget for and therefore requires appropriate financial controls (see section 12.3):
 - For Infrastructure (IaaS) this is usually based on a combination of the amount of processing and storage used, the time that it is ‘powered on’ and the amount of data uploaded or downloaded to/from the cloud provider.
 - For Software (SaaS) this is usually based on the number of users of the service and the level of service they require. For example, an Office 365 user who requires a basic email service only will pay significantly less per year/month than a user who requires a larger mailbox, conferencing facilities, file storage, etc.
- **Scalable / elastic resources** - allowing customers to buy more features/compute power / storage for a period of time to deal with a short term increase in demand. Some examples include:
 - Where Infrastructure as a Service (IaaS) is used to provide a disaster recovery (DR) facility a customer can quickly switch users over to the DR system. The customer would only pay for the increased compute power and network traffic for that period of time.
 - Where Software as a Service (SaaS) is used for data analytics and a short term increase in storage or compute power is needed, this can quickly be scaled up/down.
- **‘Infinite’ resources** - the cloud provider ensures there is always capacity to deal with demand. Therefore customers do not need to concern themselves with the underpinning server infrastructure used to deliver the cloud services.
- **Incremental, continual updates with access to latest software tools** - cloud providers deliver rapid releases with small incremental increases in functionality. As this is a continual process it typically requires less user training. Users do not have to wait for ‘upgrades’, which is usually the case where software is purchased and hosted on-premises. For Software as a Service (SaaS), this is probably the main benefit, and can be of particular benefit when accessing the latest data mining and analysis tools and techniques.
- **Accessible by default** - as cloud services are typically designed to be accessible by default from anywhere with an internet connection, this enables organisations, and their workforce, to employ more flexible ways of working. This applies predominately to Software (SaaS)
- **Robust cyber security** - larger cloud providers, such as Amazon, Microsoft and Google, employ teams of dedicated cyber attackers and defenders whose purpose is to ensure that their services are as robust and secure as they can be. This often provides customers with security controls which are stronger than those that can be afforded by enterprise organisations, such as NHS Boards. In addition, security patches can be managed more effectively than on premises solutions especially where IT resources are scarce. The latest highly publicised cyber-attacks were

Information Security Policy – Cloud Computing

targeting systems that had not been updated in line with manufacturer's recommendations, i.e. Microsoft security patches.

- **Managed infrastructure** - the 'Platform as a Service' (PaaS) model provides a complete and managed platform for users to deploy their applications onto. As a result customers benefit from a reduction in the necessary resource/effort to support the environment yet have an environment that always remains up to date and fully supported.
- **Technical refresh** –hardware refreshes are the responsibility of the cloud provider. In contrast, with on premises services hardware typically needs to be replaced every five years by the customer within capital refresh programmes. More often than not this requires operating system and application updates which not only come with capital funding consequences, but also require resources to maintain safe services.

12.3 Concerns and Challenges Regarding the Use of Cloud Computing

When considering the use of cloud computing, it is important to understand the potential challenges in order to identify whether they are relevant, and if so, how they can be managed. Some of the key concerns and challenges regarding the use of cloud computing are identified below.

- **Control over information / data**
When a cloud provider is used to deliver a service, some of the control over the information/data held transfers to that third party provider and their staff. Many of the leading cloud providers design their systems and control mechanisms to segment systems to actively prevent access for their staff. In order to protect access to the data/systems, suitable contractual controls should be put in place between the customer and the cloud provider to ensure that the necessary level of control is provided. These controls need to be included within the terms and conditions and specifications of the Agreements and must be proactively managed throughout the life of the contract.
- **Location of data held**
When a cloud provider is used, control over where the data is held can be lost. Some cloud providers may store or process data offshore, and it is possible to have numerous jurisdictions apply to data held in cloud services. When data is transferred outside of the European Union, the customer needs to ensure that appropriate controls are in place to protect the data. Some of the larger cloud providers including Microsoft and Amazon have UK specific data centres which help meet this requirement.
- **Funding – capital vs revenue**
Cloud services normally require revenue funding as they are a managed service agreements, however IT equipment in NHS Lanarkshire is capital funded. As such, a move to cloud computing will require a shift from a capital funded model to a revenue funded model – this should be factored in/considered at the business case stage.

Information Security Policy – Cloud Computing

- **Funding – variable costs**

As cloud services are 'pay as you use', the costs can be unpredictable, with the level of unpredictability depending upon the type of service being consumed. For example, SaaS with per-user pricing is very predictable, whereas IaaS has more variability. Time and effort should be allocated up front to assess potential levels of usage as accurately as possible to enable more accurate costs to be included within the business case; however it should be made clear in the business case that actual costs may vary over time. It is therefore essential that appropriate provisions should be made within any subsequent contractual agreements to ensure that value for money is secured via an appropriate discount structure and any other commercial benefits. Costs should then be regularly reviewed throughout the life of the contract.

- **Security**

Many cloud delivered services are designed to support a modern mobile workforce and as such are accessible directly over the internet, by default. As with on-premises delivered services, cloud services are highly configurable and the detailed security configuration will be down to the customer. As such, careful configuration and testing is needed to ensure that all cloud services are designed and configured with appropriate security controls for NHS Lanarkshire use.

- **Public perception**

While appropriate legally enforceable Information Governance and Security controls will need to be in place when using cloud services, the public's perception of the NHS using cloud services to store and process their data will need to be carefully considered.

- **Supplier tie-in**

As commercial entities, cloud providers may offer many incentives to encourage adoption of their products and services which may result in a degree of 'lock-in' with the cloud provider.




The following must be considered and written into the contract's terms and conditions prior to entering into any agreement with a provider:

- Exit costs where appropriate – these should be identified, agreed and documented.
- Vendor neutral components – these should be used as standard and any derivation from this should be appropriately assessed and documented and a plan for exit developed which needs to be updated throughout the term of the agreement.
- Data migration - the technical feasibility of extracting data and migrating it to another supplier should be assessed. Consideration should be given to design costs, data migration, time required and costs for any supplier assistance/consultancy.


Information Security Policy – Cloud Computing

13. [Appendix 3 - NHS Digital Guidance on the Use of Cloud Services](#)

The NHS Digital/Department for Health guidance has been designed specifically to consider the risks associated with the storage and processing of NHS data types and comprises the documents in the table below. They are available from [NHS Digital: NHS and social care data: off-shoring and the use of public cloud services](#).

NHS Digital Guidance: NHS and social care use of public cloud services	<p>This guide explains the safeguards that must be put in place to do so, including considerations about where the data can be located.</p>  <p>guidance_on_nhs_and_social_care_use_</p>
Health and Social Care Cloud Security - one page overview	<p>This is a single sheet, aimed at data controllers, which summaries the approach and gives details of the steps to be followed when assessing the use of cloud services.</p> <ul style="list-style-type: none"> • Understand the data you are handling • Assess the risks associated with the data • Implement proportionate controls • Monitor
Health and Social Care Cloud Risk Framework	<p>This is a framework for assessing and managing the risks around the use of public cloud technologies. It enables a consistent assessment of the risks and helps organisations to understand where their use of public cloud facilities aligns with their own risk appetite.</p>  <p>cloud_risk_framework_document_final.p</p>
Health and Social Care Data Risk model	<p>This is a tool which can be used to quantify the level of risk presented. It takes into consideration 3 main factors:</p> <ul style="list-style-type: none"> ○ The type of data ○ The scale ○ Its level of persistency <p>The output of the tool is a risk profile class ranging from I to V. Pre-defined acceptability criteria can then be considered in relation to the identified risk profile.</p>  <p>health_and_social_care_data_risk_model</p>
Health and Social Care Cloud Security- Good Practice Guide	<p>This supplements the framework and provides detailed technical advice regarding the controls that are required (both by the customer and also the provider) dependent upon the previously calculated risk profile. Suppliers should be provided the NHS Digital Health and Social Care Cloud Security Good Practice Guide spread sheet, along with the identified risk profile produced in Step 1. The supplier needs to complete this spreadsheet with details of the technical controls to meet the requirements.</p>

Information Security Policy – Cloud Computing

	<p> </p> <p>cloud_security_goo cloud_security_goo d_practice_guide_fir d_practice_guide_fir</p> <p>The controls are based on the advice published by the NCSC NCSC Guidance on Implementing the Cloud Security Principles</p>
--	---

Uncontrolled when printed