NHS and social care data: off-shoring and the use of public cloud services

NHS and social care organisations can safely locate health and care data, including confidential patient information, in the public cloud including solutions that make use of data off-shoring.

This guide explains the safeguards that must be put in place to do so, including considerations about where the data can be located.

In brief:

- NHS and Social care providers may use cloud computing services for NHS data. Data must only be hosted within the European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield.

- Senior Information Risk Owners (SIROs) locally should be satisfied about appropriate security arrangements (using National Cyber Security Essentials as a guide) in conjunction with Data Protection Officers and Caldicott Guardians.

- Help and advice from the Information Commissioner's Office is available and regularly updated.

- Changes to data protection legislation, including the General Data Protection Regulation (GDPR) from 25 May 2018, puts strict restrictions on the transfer of personal data, particularly when this transfer is outside the European Union. The ICO also regularly updates its GDPR Guidance.

Use of cloud computing services

1) The UK Government introduced a 'cloud first' policy for public sector IT in 2013. The use of cloud services was also endorsed in the National Information Board's Personalised Health and Care 2020 framework, published in November 2014

and, if implemented correctly, it is compliant with the National Data Guardian's recommendations.

2) Provided that the upmost care is taken when collecting, transferring, storing and processing patient data, NHS and social care organisations are permitted to host data within the UK, EEA (countries deemed by the European Commission to have adequate protections for the rights of data subjects), or in the US where covered by Privacy Shield.

3) There are no restrictions on where in the UK data may reside, for example data from the NHS in England data may be hosted in Scotland, and vice versa. (See 'Further detail on acceptable locations for data offshoring' at foot of page)

What is cloud computing?

4) As defined by the National Institute of Standards and Technology: "Cloud computing is a model for enabling ubiquitous, 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."

5) Public cloud services, defined as cloud infrastructure provisioned for open use by the general public, offers the biggest potential benefits for the public sector. There are other deployment models available such as community, hybrid or private cloud.

6) NHS and social care organisations can safely put health and care data, including non-personal data and confidential patient information, into the public cloud. Many NHS organisations and government departments have already made this decision based on risk management assessments and having put appropriate safeguards in place.

Benefits of the cloud

7) Cloud providers have a significant budget to pay for updating, maintaining, patching and securing their infrastructure. This means cloud services can mitigate many common risks NHS and social care organisations often face.

8) Cloud services may provide other advantages for NHS and social care organisations including lower IT costs and the ability to develop, test and deploy services quickly without large capital expense.

9) As more services for patients and staff move to the Internet and the need for better data interoperability increases, it is likely that use of cloud services will become more prevalent in NHS and social care organisations.

Migrating to the Cloud: four steps to informing a risk-based decision

10) All decisions relating to the security of data are the responsibility of the local data controller within a healthcare organisation. In accordance with recommendations made by the National Data Guardian, organisations should also have a SIRO responsible for data and cyber security who should be included in making a risk-based decision.

11) Well-executed use of cloud services is appropriate for most NHS and social care information and services. However, your organisation may have different needs, dependent on your data security requirements. These requirements will be defined by the availability, integrity and confidentiality criteria of your specific data or systems.

12) However, there are some potential downsides to cloud services that need to be considered when making a risk-based decision:

a) Moving critical services to the cloud will increase the importance of Internet access to your organisation. If your Internet access is disrupted or is unreliable, you may lose access to your data and services.
b) You may need to change the way you budget for technology as cloud services usually operate on a pay-as-you-go (revenue) model rather than capital expenditure.
c) You may need to recruit the right capability to deliver and manage cloud services if your organisation has no prior experience of running this type of service.
d) Not all systems were designed to run in the cloud, and so some may not be compatible.
e) Use of the cloud increases the portability of data, meaning data can be distributed across multiple devices both within and without the boundary of your organisation. The right cultural understanding and behaviours need to be in place to manage this portability appropriately mitigate any risks.

13) You should take into account these and other relevant factors, including, but not limited to, cost, security, resilience, capability and funding when deciding whether to use cloud services. If you are unsure, seek specialist advice.

14) These are the steps you should take to ensure you select and implement a solution that is appropriate for the risk level of the specific data set or system your organisation has decided to move to the cloud.

Step 1: Understand the data

15) All data managed by NHS and social care organisations should be treated as OFFICIAL data, in line with the Government Security Classification Policy.

16) However, you shouldn't treat all information equally. All information in your organisation will need risk-appropriate and proportionate security measures based on the service level of the system, the type of data you are dealing with, how much of it there is, and how long you will be retaining the data for.

Step 2: Assess the risks

17) Once you have gathered this information about the data or system you are considering moving into the cloud, you can use it to classify your data based on its level of risk.

18) There are a number of risk models available for classifying data and you should choose the one that is most appropriate for you and your organisation. If you are unsure of what factors the model should take into account when assessing your data, you can refer to:

    a) the National Cyber Security Centre's guidance on making risk based decisions
    b) the NHS Digital Health and Social Care data risk framework.

19) As an organisation, you retain Data Controller responsibility. It is possible that, once you have completed your risk assessment process, by following steps such as those outlined here, there may be some situations where cloud services are deemed not appropriate for specific systems or data. You will also want to refer to the European Union General Data Protection Regulation (GDPR), and how you can ensure privacy by design and conduct the necessary data protection impact assessments.

Step 3: Implement controls (data protection and location)

20) Assessing your data on a case-by-case basis is important because even though the cloud provider will be responsible for various elements of hosting and maintenance of a data, your organisation will retain data controller responsibilities

and is therefore, ultimately, responsible for ensuring that proportionate security controls are put in place to mitigate all risks.

21) There are a number of pieces of relevant legislation and policy to help inform these proportionate decisions. These are:
    a) The Government Security Classification Policy;
    b) The Data Protection Act and EU General Data Protection Regulation (GDPR); and
    c) The Information Governance Toolkit v14.1, which will be superseded by The Data Security and Protection Toolkit from April 2018.

22) In general, these requirements are universal and large cloud service providers should have taken these into account when producing standard contractual terms. For example it is normal for contracts to include specific clauses relating to data availability, resilience and recovery. However, this is not a given and you may also have more specific requirements that you will want to ensure are built into the contract with your cloud provider, based on your risk assessment of the data. To help you define these requirements, you should talk to your cloud provider but also refer to:

    a) The Information Commissioner's Office (ICO) guidance for organisations considering using cloud services to process personal data;
    b) The ICO guidance on data protection reform (GDPR);
    c) NHS Digital's Cloud Security Good Practice Guide; and
    d) The National Cyber Security Centre's 14 Cloud Security Principles

23) These requirements will also influence, and be influenced by, where your cloud provider is processing or storing your data, as you may choose to take advantage of cloud solutions that conduct these functions outside of the UK.

24) Considering cloud providers that host or process data within EEA or adequate countries can be beneficial as it gives you more choice over cost, availability and resilience. To benefit from additional resilience it is highly recommended that for the data you deem to be of the highest risk you consider taking a multi-region approach; where, for example the data is stored both in and outside of the UK.

25) It is important to remember that these are legally complex considerations. It is possible to have numerous jurisdictions apply to data held in cloud services, (particularly when the cloud provider is non UK, or has a non UK parent company). Whilst Cloud providers should let you specify geographic region(s) to host or process data, you should clarify before contracting out. Furthermore, service providers sometimes use offshore technical and support staff, who are able to access data from another location. Many global service providers have a

global support model that does not limit where staff can operate. You will want to understand whether this has any impact for your risk-based decision.

26) When selecting a cloud provider you should ask them to provide clarity on these complexities and their ability to meet all of your security requirements, not just those related to the National Security Centre's 14 principles - evidence of which is detailed for each provider listed on the Digital Marketplace.

27) Finally, in addition to these quantitative measures you should explain to your service users how you are storing and managing their personal confidential data. Some people may associate 'the cloud' with the consumer Internet services they are familiar with (e.g. email, file sharing), rather than the securely designed enterprise cloud services used by many organisations.

28) If you are unsure about what any of this means for your organisation, seek legal advice.

Step 4: Monitor the implementation

29) As stated, whilst your cloud provider will have data protection responsibilities as a data processor, your organisation will retain data controller responsibilities and must be assured at all times that the selected cloud implementation is fit for purpose. Your organisation's security requirements will change over time, so regular review points are recommended.

30) In accordance with the recommendations made by the National Data Guardian, your organisation should have a SIRO responsible for data and cyber security. You should ensure that this individual has access to the evidence provided by your cloud provider that they are compliant with the recognised standards, which could include third party verification of this, and the additional security controls that you may have requested. This evidence and the implementation itself should be reviewed regularly to ensure that any necessary changes to your cloud solution are made in a timely fashion.

Further detail on acceptable locations for data offshoring

Hosting data in the UK, EEA or adequate countries

Personal confidential data can be hosted in countries that provide an adequate level of protection for personal data.

Principle eight of The Data Protection Act states that:

> "Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

The European Commission provides a list of adequate countries. It is the responsibility of local organisations to monitor and take note of any future changes to this list, in the case of any future amendments.

There are other mechanisms to host personal confidential data outside the EEA while satisfying the requirements of the eighth principle of the Data Protection Act - including Model Clauses in contracts and Binding Corporate Rules.

For more information you should refer to the Information Commissioner's guidance on sending personal data outside the EEA.

If you are planning to host data outside the EEA, or with a provider based outside the EEA, you should assess the impact of this data being subject to the legal jurisdiction of that country when making a risk-based decision.

Hosting data in the United States

NHS and social care data can be safely hosted with certain organisations in the US.

Personal confidential data can be hosted with organisations that participate in the Privacy Shield scheme agreed between the EU and US. The European Commission has issued a formal decision that the Privacy Shield provides adequate protection to allow personal data to be transferred to the US.

If you are planning to host data with an organisation in the US, you should verify whether they are part of this scheme on the Privacy Shield website, and whether the type of data you plan to transfer is covered by the organisation's Privacy Shield commitments.

If the organisation you plan to host data with is not part of the Privacy Shield scheme, you will not be protected by the agreement. You should seek legal advice if you plan to host personal confidential data with a US provider that is not part of the Privacy Shield.

There are other mechanisms to host personal confidential data in the US while satisfying the requirements of the eighth principle of the Data Protection Act - including Model Clauses in contracts and Binding Corporate Rules.

For more information you should refer to the Information Commissioner's guidance on sending personal data outside the EEA and transferring data to the US.

Hosting data in other countries

NHS and social care organisations are not expected to host data outside of the UK, EEA, US or adequate countries as determined by the European Commission.