Follow these steps to safely use public cloud in the health and social care system

It is always appropriate to consider the use of public cloud when designing and implementing any kind of information system. This guidance supports you in your role as Data Controller, ensuring that all uses of public cloud are well-executed: known, safe, secure and effective. The Health and Social Care Cloud Security Good Practice Guide provides detailed guidance.

1. **Understand** *the data you are handling*

- Get a list of all the data types/attributes that will be stored / processed by the system.
- How much data is under consideration?
- How long will it be held in the system?
- What is the Service Classification of the system (Bronze | Silver | Gold | Platinum)?
- Carefully assess the data types/attributes and decide which data types this relates to. Use the Risk Model to obtain a Risk Classification.

Refer to:

- Health and Social Care Cloud Security Good Practice Guide
- Health and Social Care Cloud Risk Framework
- Health and Social Care Data Risk Model

Document:

- Retain the list of data types/attributes.
- Record the rationale for selecting the data type(s).
- Retain the completed risk model.

2. **Assess** *the risks associated with the data*

- Does the calculated risk classification align with your organisation's risk appetite? Undertake appropriate governance to ratify.
- Other considerations:
  - ➢ Consider breaking down complex systems and using the public cloud for specific subsystems.
  - ➢ As-Is situation – an existing 'high-risk' implementation may be better in the cloud than how it's currently hosted.
  - ➢ Public perception -You must be comfortable with any challenge that comes from the public and the media.
  - ➢ Lock-in and Migration - using vendor specific components will make it harder to migrate to another provider
  - ➢ Requirements - Are there any technical limitations or specific requirements that may preclude the use of public cloud?
  - ➢ Impact of breach - consider the impact and subsequent management of any unintended breach

Refer to:

- Health and Social Care Cloud Risk Framework.

Document:

- The governance decision to use the cloud (e.g. meeting minutes).
- Responses to all other considerations.

3. **Implement** *proportionate controls*

- Apply proportional controls:-
  - ➢ Select a Cloud provider that meets the required security standards – those that match the security and service classification.
  - ➢ Apply the security controls that are under your responsibility – those that match the security and service classification.

Refer to:

- Health and Social Care Cloud Security Good Practice Guide

Document:

- Evidence that the supplier meets the standard.
- Evidence that you have implemented the controls.

4. **Monitor**

- Ensure that your vendor keeps you informed of any changes that may affect, in a detrimental way, the security of your system and data.
- The security controls that you have implemented need to be reviewed and audited on a regular basis.

Document:

- Waivers / residual risk.
- Revised certifications and assessments.