UK Healthcare and Life Sciences Compliance on AWS

January 4th, 2023

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This whitepaper is intended to provide an overview of the UK Government's approach to public cloud usage and an understanding of the core governing bodies, policies, and technical approaches taken by public and commercial customers, and to address other key areas of discussion. Amazon Web Services (AWS) has developed the content-based on experience with and feedback from our Healthcare and Life Sciences (HCLS) customers and AWS Partners who are currently running UK HCLS-compliant workloads on AWS. This whitepaper will further outline how AWS addresses UK-focused compliance and security questions through correct use of AWS services. The document does not provide legal guidance or claim to cover the entirety of the questions or challenges customers may face.

Introduction

This document provides a high-level overview of the UK Government's approach to public cloud usage. This guide will help to provide you with the information startups need to begin your compliance journey with AWS. This information is intended to give you an understanding of the core governing bodies, policies, and technical approaches taken by both public and commercial customers, and to cover other key areas of discussion with your customers.

When dealing with healthcare data in the United Kingdom, organizations will likely need to ensure they are following the UK Data Protection Act (for guidance, visit the UK Information Commissioner's Office website).

The UK health industry's use of the public cloud is guided by the documents on the NHS and social care data: off-shoring and the use of public cloud services website. These documents have been created and presented jointly by the Department of Health and Social Care (UK), National Health Service (NHS) Digital, NHS England, and NHS Improvement. To summarise, this document allows organisations that follow these guidelines to store and process confidential patient health information. Organisations should store health data in the UK or in a country that is covered under UK *adequacy regulations* (for example, an European Economic Area (EEA) country); however, if organisations propose to store or transfer the data to a country where no adequacy decision is in place, then those organisations must put in place appropriate safeguards under the UK Data Protection Act.

NHS and social care organisations can 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.

Additionally, all organisations that have access to NHS patient data and systems must use the Data Security and Protection Toolkit (DSP Toolkit) to provide assurance that they are practising good data security and that personal information is handled correctly. The toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

The DSP Toolkit matrix references particular areas in which you can use AWS services to help meet common compliance requirements. Later in this whitepaper, you will be able to see the AWS services that are commonly used by AWS HCLS customers.

AWS data privacy

At AWS, customer trust is our top priority. AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might need to meet their compliance needs. Maintaining customer trust is an ongoing commitment. We strive to inform you of the privacy and data security policies, practices, and technologies we've put in place. Our commitments include:

Access. As a customer, you maintain full control of your content that you upload to the AWS services that are enabled in your AWS account, and responsibility for configuring access to AWS services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (for example, AWS Identity and Access Management (IAM), AWS Organizations and AWS CloudTrail). We provide APIs for you to configure access control permissions for any of the services you develop or deploy in an AWS environment. We do not access or use your content for any purpose without your agreement. We never use your content or derive information from it for marketing or advertising purposes.

Storage. You choose the AWS Region(s) in which your content is stored. You can replicate and back up your content in more than one AWS Region. We will not move or replicate your content outside of your chosen AWS Region(s) without your agreement, except as necessary to comply with the law or a binding order of a governmental body.

Security. You choose how your content is secured. We offer you industry-leading encryption features to protect your content in transit and at rest, and we provide you with the option to manage your own encryption keys. These data protection features include:

- Data encryption capabilities available in over 100 AWS services.
- Flexible key management options using AWS Key Management Service (AWS KMS). This allows customers to choose whether to keep complete control over their encryption keys or have AWS manage their keys.

Disclosure of customer content. We will not disclose customer content unless we're required to do so to comply with the law or a binding order of a government body. If a government body sends AWS a demand for customer content, we will attempt to redirect the government body to request that data directly from the customer. If compelled to disclose customer content to a government body, we will give customers reasonable notice of the demand in order to allow the customer to seek a protective order or other appropriate remedy, unless AWS is legally prohibited from doing so. See our Law Enforcement Information Requests page for up-to-date reports on these requests.

Security Assurance. We have developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

Overview of UK healthcare regulation with relation to AWS

When reviewing the UK government's approach to the cloud, there are a number of key considerations:

- Cloud first policy
- UK Data Protection Act
- Guide to the UK GDPR
- ISO/IEC 27001

Cloud first policy

The UK Government introduced a 'cloud first' policy for public sector IT in 2013. This policy states that when procuring new or existing services, public sector organisations should consider and fully evaluate potential cloud solutions first before considering any other option. This approach is mandatory for central government and strongly recommended to the wider public sector.

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 is compliant with the National Data Guardian's recommendations.

The National Data Guardian (NDG) role was created in November 2014 to be an independent champion for patients and the public when it comes to matters of confidential health and care information. The purpose of the role is to make sure that people's information is kept safe and confidential, and that it is shared when appropriate to achieve better outcomes for patients. The NDG does so by offering advice, guidance, and encouragement to the health and care system.

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 Senior Information Risk Owner (SIRO), responsible for data and cybersecurity, who should be included in making a risk-based decision.

Well-architected use of cloud services is appropriate for most NHS and social care information and services. However, the relevant organisation may have different needs, dependent on their data security requirements. These requirements will be defined by the availability, integrity, and confidentiality criteria of their specific data or systems. The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud, which can help to meet a number of these requirements.

Some of the benefits of using AWS are:

- AWS invests heavily in the architecture and services it provides on an ongoing basis. This investment can help customers mitigate many common security risks faced by the NHS and other social organisations.
- Organisations can lower their IT costs and develop, test, and deploy services quickly without large capital expense, in particular when using managed services.
- The AWS shared responsibility model simplifies the process of assessing and addressing risks. For example, when following the recommendations for UK businesses from the National Cyber Security Centre's guidance, customers can use AWS to directly enforce some of the principles (like asset protection and resilience or supply chain security) while they use AWS security features to enforce the principles that customers are responsible for. AWS has a broad customer base that hosts compliant workloads on AWS across all sectors, meeting UK Government requirements.

In addition to these benefits, AWS operates the AWS Risk and Compliance Management program. This program aims to manage risk in all phases of service design and deployment and to continually improve and reassess the organization's risk-related activities. AWS also participates in the voluntary Cloud Security Alliance (CSA), an independent organisation that is dedicated to defining and raising awareness of best practices, to help ensure a secure cloud computing environment. There are two resources available to customers that document the alignment of AWS to the CSA Consensus Assessments Initiative Questionnaire (CAIQ). The first is the CSA CAIQ whitepaper, and the second is a more detailed mapping to our SOC-2 controls, which is available through AWS Artifact. For more information about the AWS participation in CSA CAIQ, see the AWS CSA website.

Other factors to take into consideration when you decide whether to use cloud services include, but are not limited to, cost, security, resilience, capability, and funding. Where unsure, seek specialist advice.

For those customers looking to build a thorough and comprehensive plan for how to adopt the cloud, there are two other frameworks to reference:

- The AWS Cloud Adoption Framework (AWS CAF) is designed to help organizations develop and implement efficient and effective plans for their cloud adoption journey (including security and compliance). The guidance and best practices provided by the framework help you build a comprehensive approach to cloud computing across your organization, and throughout your IT lifecycle.
- The AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. Built around six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—AWS Well-Architected provides a consistent approach for cloud users and partners to evaluate architectures and implement scalable designs. The security pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, managing user permissions, and establishing controls to detect security events.

Private sector regulatory considerations

Private hospitals and clinics are not governed by the same rules as their NHS counterparts, however they do still have a legal obligation to meet the minimum standards of quality and safety that their patients should reasonably expect. These standards are upheld by the Care Quality Commission in England, as well as Healthcare Improvement Scotland, the Healthcare Inspectorate Wales, and the Regulation and Quality Improvement Authority in Northern Ireland. These bodies are supported by a number of other organisations.

The Care Quality Commission

The Care Quality Commission (CQC) inspects every private hospital and clinic in England at least every two years to assess how they measure up to the standards described previously. They can also visit more often if prompted by complaints. The Care Quality Commission publishes the results of every inspection online, in the public domain, so that the standards of care and safety are laid bare for all to see. The CQC also has powers to take action if these standards fall short of what is expected. These powers fall into two categories:

- **Compliance actions** – Where the CQC will recommend a course of action to bring the hospital or clinic up to the required standard. These actions will be agreed with the facility, and the CQC will monitor their implementation to ensure that the action is taken and that it achieves the desired results.
- **Enforcement actions** – Under the Health and Social Care Act 2008, the CQC has the power to prosecute hospitals or clinics which continue to fail to meet the required standards, despite the intervention of compliance actions. This includes civil or criminal procedures in the courts.

The Care Quality Commission aims to work with private hospitals and clinics to help them to achieve the highest standards, rather than merely act as a regulator and punish offenders.

The Health and Safety Executive

The Health and Safety Executive (HSE) also has a role in regulating private hospitals and clinics by ensuring that minimum standards are met for the protection of both staff and patients. The HSE does not get involved in matters of care quality or treatment outcomes, but it does regulate matters regarding the safety of the workplace and the public environment.

Medicines and Healthcare products Regulatory Agency (MHRA)

The Medicines and Healthcare products Regulatory Agency (MHRA) is an executive agency of the Department of Health and Social Care in the United Kingdom which is responsible for ensuring that medicines and medical devices work and are acceptably safe.

The MHRA 'GXP' Data Integrity Guidance and Definitions document provides guidance on the data integrity expectations that should be considered by organisations involved in any aspect of

the pharmaceutical lifecycle, or involved in Good Laboratory Practices (GLP) studies that are regulated by MHRA.

Since the release of the MHRA data integrity guidance in March 2018, the Organisation for Economic Co-operation and Development (OECD) has issued an Advisory Document on Data Integrity (released 20 September 2021) which takes precedence over the MHRA data integrity guidance, due to the UK's membership in the OECD Mutual Acceptance of Data System.

Good Laboratory Practice (GLP)

The MHRA provides guidance on GXP data integrity. This link also provides GXP guidance on AWS. *GXP* refers to the various good practices regulated by the UK MHRA, including the Good Laboratory Practice Monitoring Authority (GLPMA). These are Good Clinical Practice, Good Distribution Practice, Good Laboratory Practice, Good Manufacturing Practice, and Good Pharmacovigilance Practice. The GXP data integrity guidance has a high degree of alignment with documents published by other regulators, such as PIC/S, WHO, OECD (guidance and advisory documents on GLP) and EMA. It is designed to facilitate compliance through education, whilst clarifying the MHRA's position on data integrity and the minimum expectations to achieve compliance.

Getting started

All organizations, public or private, which have access to NHS patient data and systems must use the DSP Toolkit to provide assurance of compliance. The DSP Toolkit is an annual self-assessment. As data security standards evolve, the requirements of the Toolkit are reviewed and updated to ensure they are aligned with current best practice. Organisations with access to NHS patient data must therefore review and submit their DSP Toolkit assessment each year before the deadline. The DSP Toolkit also provides organisations with a means of reporting security incidents and data breaches.

Completion of the DSP Toolkit is a contractual requirement specified in the NHS England Standard Conditions contract, and it remains the policy of the Department of Health and Social Care that all bodies that process NHS patient information, for whatever purpose, provide assurances by using the DSP Toolkit. Completion of the DSP Toolkit is also necessary for organisations which use national systems such as NHSmail and the e-referral service.

The first time you register and log in to the DSP Toolkit portal, you will be asked to choose the most appropriate sector for your organisation, to provide details of key roles, and whether you have any relevant certifications. This is called the *Organisation Profile*. The answers you give here will tailor the questions you need to respond to in your self-assessment. Guidance on selecting the correct organisation type for your organisation can be found on the DSP Toolkit Help page. Information regarding the DSP Toolkit Standard and a full list of the 2021/22 requirements for all organisation types are provided on the News page. The requirements for the DSP Toolkit are tailored to your organisation type.

Cyber Essential Plus and ISO 27001 certifications can be used to reduce the number of evidence items to complete. The evidence items those certifications will cover can be evaluated for each item by consulting the *DSP Toolkit Evidence Items, Exempt for ISO27001*, and *DSP Toolkit Evidence Items Exempt for Cyber Essentials PLUS* columns in the DSP Toolkit requirements list.

The Data Security Meta Standard is a useful resource that can help you understand the coverage each of those certifications provide against the DSP Toolkit assertions and evidence items. The ISO 27001 certification provides significant coverage and represents a structured way to meet the DSP Toolkit standards. ISO 27001 is also a worldwide industry-recognized certification and often represents the foundation of other countries' HCLS compliance programs, too. The ISO 27001 certification alone will not cover all DSP Toolkit requirements, and its coverage can be assessed from the Data Security Meta Standard and the DSP Toolkit requirements list.

You can use other certifications, like the Cyber Essential Plus and Public Services Network (PSN) compliance, to reduce the number of evidence items to cover. Consult the NHS Data Security Meta Standard document for further details.

Independently of the path you choose to meet the NHS DSP Toolkit standards, AWS offers services, features, and support that can help you effectively build, maintain, and document a secure and compliant solution.

In particular, we list in this section seven of the 10 National Data Guardian's (NDG's) security standards that the DSP Toolkit requirements are based on and describe how AWS can help you to meet these standards. In this whitepaper, we will cover the Process and Technology standards. Customers should review all of the NDG security standards to ensure they are meeting the requirements, as many apply at the organisation level.

Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses, by following these recommendations:

- Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
    - Use services such as AWS Directory Service, Amazon Cognito, AWS Identity and Access Management (IAM) and IAM Identity Center (successor to AWS Single Sign-On) to manage data, service, and application access. Those services make it convenient to adopt security best practices like least privilege permissions and multi-factor authentication (MFA), and to enforce password policies.
- Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
    - Use services such as Amazon Detective, Amazon CloudWatch, AWS CloudTrail, AWS Config and Amazon VPC Flow Logs to provide advanced auditing and logging to support root cause analysis. These services provide the following capabilities:
        - Amazon Detective simplifies the task of network flow analysis by security analysts.
        - Amazon CloudWatch monitors the AWS environment and generates alerts similar to a Security Information Event Management (SIEM) system, which can be ingested into a customer's on-premises SIEM.
        - With AWS CloudTrail you can monitor your AWS deployments in the cloud by getting a history of AWS API calls for the account, including API calls made through the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services like auditing bucket and object-level requests on Amazon S3. CloudTrail can identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred.
        - AWS Config maintains a configuration history of your AWS resources and evaluates the configuration against best practices and your internal policies. You can use this information for operational troubleshooting, audit, and compliance use cases.

- Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.
- AWS Security Hub provides a comprehensive view of the security state within AWS and your compliance with security standards and best practices. It collects, centralizes, and prioritizes findings from the security services and supported third-parties enabled across your AWS accounts to help you analyse your security trends and identify the highest-priority security issues.

- Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection (this is not an AWS requirement and it is customer responsibility to comply with it).
  - Use AWS Security Hub to collect and notify security events. You can also use Amazon WorkSpaces to provide consistent, secure and flexible virtual desktops and use our numerous partners on the AWS Marketplace to deploy antivirus and anti-malware solutions. Such solutions strengthen local and remote workforce security posture by storing user data on AWS instead of on vulnerable endpoint devices. You can use AWS Network Firewall to enforce outbound traffic filtering and help protect users from accessing malicious websites. Amazon Simple Email Service (Amazon SES) can help protect email systems from email spoofing and its features enable compliance with DMARC (Domain-based Message Authentication, Reporting, and Conformance), DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) security frameworks. To protect your external facing services against DDOS, you can use AWS Shield and AWS WAF. AWS Shield has two tiers: AWS Shield Standard, which is automatically enabled to all AWS customers at no additional cost, provides protection against common and most frequently occurring infrastructure (layer 3 and 4) attacks like SYN/UDP floods, reflection attacks, and others to support high availability of your applications on AWS. AWS Shield Advanced provides additional protections against more sophisticated and larger attacks for your applications running on Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53. Instead AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define.
  - Use the AWS Security Incident Response Guide as a resource to understand cloud security and incident response concepts. The guide identifies cloud capabilities, services, and mechanisms that are available to customers who are responding to security issues. In the guide, a holistic approach is presented that covers people, processes, and technologies that help achieve strong incident response capabilities.

Technology: Ensure technology is secure and up-to-date by following these guidelines:

- No unsupported operating systems, software or internet browsers are used within the IT estate.
    - AWS Systems Manager Inventory can help build a software and hardware inventory (including configuration) across Amazon Elastic Compute Cloud (Amazon EC2) and on-premises computing environments. Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed instances with both security related and other types of updates. The service can be used to patch fleets of Amazon EC2 instances or on-premises servers and virtual machines (VMs) by operating system type.
    - AWS Service Catalog allows IT administrators to create, manage, and distribute catalogues of approved products to end users, who can then access the products they need in a personalized portal. Administrators can control which users have access to each product to enforce compliance with organizational business policies.
    - You can also rely also on the vast AWS Partner Network for strategic experts and experienced builders and the AWS Marketplace for third-party solutions. The third-party security solutions available in AWS Marketplace complement existing AWS services to help you deploy a comprehensive security architecture and a more seamless experience across your AWS environments.
- A strategy is in place for protecting IT systems from cyber threats, which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
    - The numerous AWS security services and features minimize the burden to implement cybersecurity frameworks and achieve compliance with certifications like Cyber Essentials or ISO 27001. As explained in the AWS shared responsibility model section later in this paper, this model can help relieve your operational burden because AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.
    - AWS WAF protects your web applications from common web exploits and can be used to address the top application security flaws as named by the Open Web Application Security Project (OWASP). You can find further details in this dedicated whitepaper.
    - Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. By integrating it with IAM, customers can control who in the organization can make changes to any DNS records by creating multiple roles and managing the permissions for each of these roles within the AWS account.

- Other important services AWS offers to reliably track, deploy, and monitor changes are AWS CloudFormation, AWS Cloud Development Kit (AWS CDK) and AWS Config; the first two are powerful infrastructure-as-code (IaC) tools used to define and provision infrastructure, while AWS Config and its Conformance Packs is a service that maintains a configuration history of customer AWS resources and evaluates the configuration against best practices and internal policies. With AWS Config Rules you can monitor resource configuration and check whether any change violates any of the conditions in the rules. The rules to monitor the resources created on AWS are compliant with the defined data protection policies and security controls. AWS provides collections of AWS Config rules and remediation actions in the form of conformance packs that you can deploy and customize as a single entity in an account and an AWS Region, or across an organization in AWS Organizations. Conformance packs provide a general-purpose compliance framework to help customers create security, operational, or cost-optimization governance checks by using managed or custom AWS Config rules and AWS Config remediation actions.
- You can use AWS Security Hub to simplify the operationalization of some security standards. You can investigate findings by using the Security Hub integration with Amazon Detective, and you can build automated or semi-automated remediation actions using the Security Hub integration with Amazon EventBridge.

- IT suppliers are held accountable via contracts for protecting personal confidential data they process.
  - AWS regularly completes the Data Security and Protection Toolkit annual assessment with Standard Exceeded status.
  - AWS is a registered data controller with the UK ICO. As such, AWS follows guidance as outlined in the Data Protection Act and published by the ICO.
  - Where necessary to notify customers of security and privacy events that involve AWS services, we publish security bulletins.
  - AWS's achievement of the Cyber Essentials Plus certification demonstrates our commitment to mitigate the risk from common internet-based threats, within the context of the UK Government's 10 Steps to Cyber Security. This certification is backed by industry, including the Federation of Small Businesses, the Confederation of British Industry, and a number of insurance organizations that offer incentives for businesses that hold this certification. Cyber Essentials sets out the necessary technical controls; the related assurance framework shows how the independent assurance process works for Cyber Essentials Plus certification through an annual external assessment conducted by an accredited assessor. Due to the regional nature of the certification, the certification scope is limited to the Europe (Ireland) and Europe (London) Regions. Download the London and Dublin AWS Cyber Essentials Plus certificate.

- AWS Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. Based on five pillars—operational excellence, security, reliability, performance efficiency, and cost optimization—AWS Well-Architected provides a consistent approach for customers and partners to evaluate architectures and implement designs that can scale over time. Using a standardized methodology, AWS and our AWS Partners will work closely with your team to thoroughly review your workload, resulting in a detailed report that outlines the actionable items and provides guidance on how to resolve architectural concerns.

Public sector

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

In the UK, the legal frameworks covering how patient data must be looked after and processed are the Data Protection Act (DPA) 2018, which brought the EU General Data Protection Regulation (GDPR) into law, and the Common Law Duty of Confidentiality (CLDC). Under UK GDPR, for recording and processing health and care data, both of the following must be satisfied:

- An Article 6 condition – for personal data
- An Article 9 condition – for health data, as a special category of data

You can read more about GDPR on the Information Commissioner's Office (ICO) website.

NHS and social care organisations are permitted to host data within the UK, a country that is covered under UK "adequacy regulations" (for example, an EEA country), or other countries, provided that appropriate safeguards are put in place, such as the Standard Contractual Clauses (SCCs) included in the AWS GDPR Data Processing Addendum (DPA). For a list of other countries covered under the UK's Adequacy Regulations, you can visit this page on the ICO website.

The AWS GDPR DPA is part of our Service Terms, which means all AWS customers and partners globally can rely on the terms of the AWS GDPR DPA (which includes SCCs) because these terms apply automatically, whenever they use AWS. AWS customers and partners who wish to transfer personal data from the UK to other countries can do so with the knowledge that AWS provides the same high level of protection in other countries as it does in the UK.

As well as this, customers who are looking to work with NHS Trusts and Hospitals are generally asked (in line with UK GDPR requirements) to conduct a Data Protection Impact Assessment (DPIA) as specified by the ICO. The ICO is a non-departmental public body which reports directly to the Parliament of the United Kingdom and is sponsored by the Department for Digital, Culture, Media and Sport.

As part of the DPIA, the customer will be asked "Is the Processor compliant with 2017/18 National Data Guardian standard 10 – supplier certification frameworks. If so, which appropriate certification(s) do they hold?". In this instance, AWS is the "Processor" and the standards that must be met are described in the following:

- AWS ISO/IEC 27001 landing page
- ISO/IEC 27001:2013 (FAQs)
- ISO/IEC 27017:2015 (FAQs)
- ISO/IEC 27018:2019 (FAQs)

- ISO/IEC 27701:2019 (FAQs)
- Cyber Essentials (CE) certification
- Cyber Essentials Plus (CE+) certification
  - CE and CE+ landing page
  - CE Readiness Toolkit
- Digital Marketplace
  - Approved AWS suppliers

MHRA's GXP Data Integrity Guide (DIG)

There are no specific certifications for GxP compliance for cloud services to date. However, the controls and guidance described by this whitepaper, in conjunction with additional resources supplied by AWS, provide information on AWS service GxP compatibility, which will assist you in designing and building your own GxP-compliant solutions.

The DIG specifically talks of the cloud and IT suppliers, stating:

> Where 'cloud' or 'virtual' services are used, attention should be paid to understanding the service provided, ownership, retrieval, retention and security of data. The physical location where the data is held, including the impact of any laws applicable to that geographic location, should be considered. The responsibilities of the contract giver and acceptor should be defined in a technical agreement or contract. This should ensure timely access to data (including metadata and audit trails) to the data owner and national competent authorities upon request. Contracts with providers should define responsibilities for archiving and continued readability of the data throughout the retention period.
>
> Appropriate arrangements must exist for the restoration of the software/system as per its original validated state, including validation and change control information to permit this restoration.

Implementing a GxP-compliant environment with AWS

There is no unique certification for GxP regulations, so each customer defines their own risk profile. Therefore, it is important to note that although this information is based on AWS experience with life science customers, you must take final accountability and determine your own regulatory obligations.

The basic principles governing on-premises infrastructure qualification still apply to virtualized cloud infrastructure. Therefore, you should still use the current industry guidance. Traditionally, a regulated company was accountable and responsible for all aspects of their infrastructure

qualification and application validation. With the introduction of public cloud providers, part of that responsibility has been shifted to a cloud supplier. The regulated company is still accountable, but the cloud supplier is now responsible for the qualification of the physical infrastructure, virtualization, and service layers and for managing the services they provide. The difference now is that there is a shared compliance responsibility model which is similar to the shared responsibility model described in this whitepaper. The customer is responsible for using the compliance documentation and understanding the services that they decide to use from the cloud provider.

For a full overview of how to implement a GxP-compliant environment with AWS, refer to the *AWS Products in GxP Systems* section in the GxP Systems on AWS whitepaper.

NHS Digital API

NHS Digital is responsible for creating digital tools and data services to support clinicians' work, patients' care, and data access to improve health and care.

NHS Digital built and provides access to different type of APIs which can be accessed by a customer's software after the customer goes through an onboarding process. The underlying technologies, protocols, security mechanisms, and onboarding processes of NHS Digital APIs can vary and sometimes can be quite long, so it is important to plan all the necessary steps well ahead of using the APIs.

The NHS Digital onboarding process for APIs provides guidance to get your software approved, while the API Catalogue provides the list of all available APIs and describes the protocol used, security and authorization procedures, the onboarding process, and networking requirements.

Private sector

As previously mentioned, all organizations which have access to NHS patient data and systems must use the DSP Toolkit to provide assurance of compliance. The DSP Toolkit is an annual assessment. As data security standards evolve, the requirements of the Toolkit are reviewed and updated to ensure they are aligned with current best practice. Organisations with access to NHS patient data must therefore review and submit their DSP Toolkit assessment each year before the deadline.

The DSP Toolkit is a composed of a set of evidence items that needs to be completed to determine if the organization is meeting the standard; such a list for 2022/2023 can be found on the DSP Toolkit website.

Each organization is mapped to a specific category, and the DSP Toolkit assessment is tailored accordingly. You can access the categorization process on the DSP Toolkit website.

You can also use Cyber Essential Plus and ISO 27001 certifications to reduce the number of evidence items to complete.

AWS shared responsibility model

Security and compliance is a shared responsibility between AWS and the customer. This shared model can help relieve your operational burden, because AWS operates, manages, and controls the components, from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. Customers assume responsibility and management of the guest operating system (including updates and security patches) and other associated application software, as well as the configuration of the AWS provided security group firewall. You should carefully consider the services you choose, because your responsibilities vary depending on the services used, the integration of those services into your IT environment, and applicable laws and regulations. The following figure provides an overview of the shared responsibility model. This differentiation of responsibility is commonly referred to as Security *of* the Cloud versus Security *in* the Cloud. These concepts will be explained in more detail in the rest of this section.

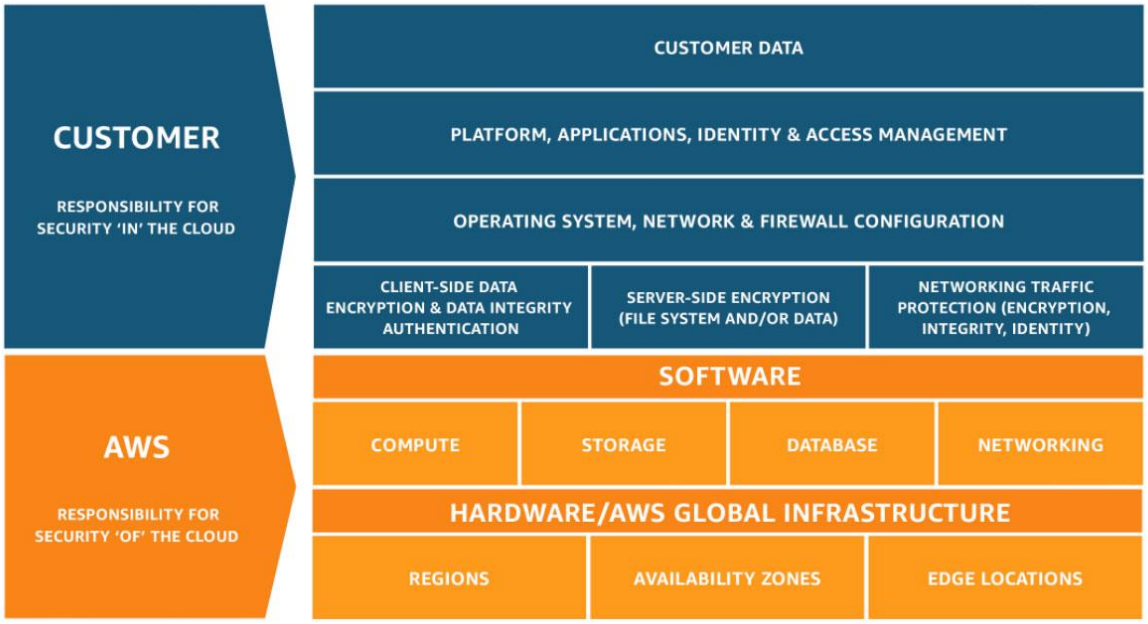

Figure 1: AWS shared responsibility model

AWS is responsible for the security and compliance of the AWS Cloud, the infrastructure that runs all of the services offered in the AWS Cloud. Cloud security at AWS is the highest priority. AWS customers benefit from a data centre and network architecture that are built to meet the requirements of the most security-sensitive organizations.

Customers are responsible for the security and compliance in the Cloud, which consists of customer-configured systems and services provisioned on AWS. Responsibility within the AWS Cloud is determined by the AWS Cloud services that you select and ultimately the amount of configuration work you must perform as part of your security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as infrastructure as a service (IaaS) and, as such, requires you to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by you on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. You are responsible for managing your data and component configuration (including encryption options), classifying your assets, and using AWS Identity and Access Management (IAM) tools to apply the appropriate permissions.

The AWS Shared Security Responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between you and AWS, so is the management, operation, and verification of IT controls shared. AWS can help to remove some operational overhead around updating, patching, and managing infrastructure, that may have been managed by you previously. Because every customer is deployed differently in AWS, you can take advantage of the ability to shift management of certain IT controls to AWS, which results in a (new) distributed control environment. You can then use the AWS control and compliance documentation available to you, as well as techniques discussed later in this whitepaper, to perform your control evaluation and verification procedures as required. Following are examples of controls that are managed by AWS, AWS customers, or both:

- Inherited controls – Controls which you fully inherit from AWS.
- Physical and environmental controls.
- Shared controls – Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure, and you must provide your own control implementation within your use of AWS services. Examples include:

- Patch management – AWS is responsible for patching and fixing flaws within the infrastructure, but you are responsible for patching your guest OS and applications.
- Configuration management – AWS maintains the configuration of its infrastructure devices, but you are responsible for configuring your own guest operating systems, databases, and applications.
- Awareness and training - AWS trains AWS employees, but you must train your own employees.

- Customer-specific controls – Controls which are ultimately your responsibility, based on the application you are deploying within AWS services. Examples include:
  - Data management – For example, placement of data on Amazon S3 where you activate encryption.

While certain controls are customer specific, AWS strives to provide you with the tools and resources to make implementation easier.

For more information about AWS physical and operational security processes for the network and server infrastructure under the management of AWS, see the AWS Cloud Security website.

For customers who are designing the security infrastructure and configuration for applications running in AWS, see the Best Practices for Security, Identity, & Compliance webpage.

AWS Cloud security

The AWS global infrastructure is designed and managed according to security best practices, as well as a variety of security compliance standards. With AWS, you can be assured that you are building web architectures on top of some of the most secure computing infrastructure in the world.

AWS certifications and attestations relating to AWS

AWS meets many of the most important security standards, see https://aws.amazon.com/compliance/programs/ for more details. The list below names a few that life science customers may find most relevant:

- SOC 1, 2, 3
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 / ISO 27701
- HITRUST (USA)
- FedRAMP
- CSA Security, Trust & Assurance Registry (STAR)

AWS provides on-demand access to security and compliance reports and select online agreements through AWS Artifact, with reports accessible through AWS customer accounts under NDA. AWS Artifact is a central resource for compliance-related information and provides additional information on the AWS compliance programs listed here.

Relevant AWS Security services

AWS offers products that fall into several categories. Following is a subset of those AWS offerings, spanning Security.

Security, Identity, and Compliance

- AWS Artifact, AWS Certificate Manager (ACM), AWS CloudHSM, Amazon Cognito, Amazon Detective, AWS Directory Service, AWS Firewall Manager, Amazon GuardDuty, AWS Identity and Access Management (IAM), AWS IAM Identity Center (successor to AWS Single Sign-On), Amazon Inspector, AWS Key Management Service (AWS KMS), Amazon Macie, AWS Resource Access Manager (AWS RAM), AWS Secrets Manager, AWS Security Hub, AWS Shield, AWS WAF

Details and specifications for the full portfolio of AWS products are available online at https://aws.amazon.com/.

Conclusion

With more than a million active customers and a global cloud presence, AWS has experience with helping organisations of all sizes migrate workloads to the cloud and deploy initially, so they can benefit from IT cost savings, improvements in productivity, business agility, and operational resilience.

This document highlights some common considerations and steps that HCLS companies should follow should they look to operate within the UK Healthcare market. Meeting these requirements set out by the UK Government will help a UK Healthcare business to successfully deploy its workloads on the AWS Cloud.

During this process, customers can use the experience and knowledge of AWS to support ongoing discussions and deployments so that their businesses can realise the benefit of using the cloud.

Contributors

Contributors to this document include:

- Camillo Anania, Senior Startup Solutions Architect, Amazon Web Services
- Will Shaw, Senior Startup Account Manager, Amazon Web Services
- Adam McCarthy, Europe, Middle East, and Africa (EMEA) Senior Startup Solutions Architect, Amazon Web Services

Document revisions

Date	Description
January 4th, 2023	First publication