Google Cloud Whitepaper
January 2023

Handling health and social data in the UK

Google Cloud

Table of contents

Disclaimer

This document was last updated in January 2023 and is for informational purposes only. Google does not intend the information or recommendations in this document to constitute legal advice. Each customer must independently evaluate its own particular use of the services as appropriate to support its legal compliance obligations.

Since Google is continually improving security and other features for our customers, some of the policies, procedures, and technologies mentioned in this document may have changed. Please visit cloud.google.com/security/compliance or contact your Google Cloud Account Representative to check for updated information.

Introduction

All organisations that have access to the United Kingdom (UK) National Health Service (NHS) health and social care data must provide assurances that they practice good information governance. This includes healthcare service providers, commissioners, and suppliers/vendors. A major part of demonstrating good information governance practices is aligning with the National Data Guardians 10 Data Security Standards.

Demonstrating how an organisation meets NHS information governance requirements can be difficult. For organisations looking to embrace cloud services and deliver scalable and innovative solutions for patients, a cloud service provider should not become an obstacle to meeting these requirements. With a trusted partner like Google as your cloud service provider, meeting your information governance requirements is easier. Google Cloud Platform (GCP) is built with security - a key component of information governance - as a core design and development principle. Google goes to great lengths to demonstrate how GCP and its underlying infrastructure can help our customers manage and safeguard data.

Google is committed to protecting our customers' data and is regularly audited by independent third-parties to verify its compliance with numerous globally recognised security and data privacy/protection standards.

In this whitepaper, we discuss the compliance landscape for UK health and social care data and, for organisations accessing patient data in England, provide an overview of NHS Digital, NHS Digital's Guidance on the use of Public Cloud Services and the Data Security and Protection Toolkit ("DSP Toolkit"). We look at the shared responsibility model for security and compliance, and examine the different roles our customers and Google have in managing these functions. We demonstrate how we have implemented the DSP Toolkit requirements and how we can help our customers meet their applicable requirements.

The compliance landscape for UK health and social care data

This section provides an overview of the legal and compliance landscape for organisations that handle UK health and social care data. It also provides an overview of the public cloud guidance and the toolkit for evidencing assurance of good information handling practices.

Legislation governing UK health data

There are many rules that govern how the health and social care data of UK citizens should be handled. Some of these rules are contained within the following legislation, and these are likely to evolve following UK's exit from the European Union:

- European Union's General Data Protection Regulation 2016/679
- UK Data Protection Act 2018
- UK Human Rights Act 1998
- UK Devolution Acts

Other rules relating to the handling of health and social care data are contained within Codes of Practice and regulatory guidance, as well as common law (judge-made law).

The key pieces of legislation are covered in more detail below.

The European Union's General Data Protection Regulation 2016/679 (GDPR)

The GDPR builds on the previous 1995 EU Data Protection Directive. It enhances data protection rights for individuals and introduces several new concepts such as the Principle of "Accountability", data protection by design and data protection by default. It also introduces new compliance obligations for organisations.

These rules apply to organisations (both inside and outside of the EU) that hold or use personal data that originates from within the EU. It also applies to organisations that carry out processing of personal data within the EU irrespective of where the individuals reside in the world.

The GDPR will continue to apply in the UK during the Brexit transition period until the end of 2020. Its role in UK law from January 2021 onwards remains unclear, as the UK's data protection regulator (the Information Commissioner's Office, or ICO) has advised that the UK will have the independence to keep the framework under review and there may be further developments regarding issues such as UK-EU transfers of personal data. The ICO advises organisations to check its website for updated guidance whenever there are developments. In any event, the GDPR is likely to remain an important influence on the UK's post-Brexit data protection laws, and so will likely remain relevant to organisations that handle UK health and social care data, particularly those with operation both in the UK and the EU.

Any organisation processing personal data must comply with the following six principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

Failure to comply with the GDPR can lead to regulatory fines and penalties. To learn more about our commitments to meeting GDPR requirements, refer to our GDPR page.

The UK Data Protection Act 2018 (DPA)

The GDPR has a direct effect across all EU member states. However, the GDPR outlines certain circumstances where member states can and must make their own provisions as to how the GDPR applies in their country. The DPA fulfills this task. It also transposes other elements of EU law (such as the EU Data Protection Directive 2016/680 relating to law enforcement) into domestic UK law. As explained in the GDPR section above, this legislation is likely to evolve following the UK's exit from the EU.

The UK Human Rights Act 1998 (HRA)

Article 8 of the HRA protects an individual's private life, their family life, their home and correspondence. This means that the state must not interfere with an individual's right to privacy and must take active steps to protect these rights. Under Article 8 there must be respect for private and confidential information, in particular the storing, sharing, and use of personal data. The HRA may evolve following the UK's exit from the EU as the UK government has indicated it might seek to repeal or replace all or part of the legislation.

The UK Devolution Acts

Some central government powers and responsibilities have been decentralised to the countries within the UK through devolution acts.[1] These acts are the Scotland Act 1998, the Northern Ireland Act 1998, and the Government of Wales Act 1998.

Through these acts, the countries above became responsible for setting policies, managing budgets and became accountable for the delivery of certain services within their territories. Health and Social Care is one of these services.

This paper focuses on NHS Digital public cloud guidance and the DSP Toolkit which applies directly in England. Although the NHS in Wales, Scotland, and Northern Ireland follow their own information governance standards with different reporting structures and organisations, many of the assurances and principles outlined in this paper may still be applicable to these countries in demonstrating compliance.

[1] Devolution of powers to Scotland, Wales and Northern Ireland

Overview of NHS Digital in England

The NHS has historically embraced technology to help deliver better services for its patients and stakeholders. NHS Digital is an executive non-departmental public body, sponsored by the UK's Department of Health and Social Care; it is tasked with several responsibilities for public health services including:

- creating and maintaining technology and infrastructure services,
- providing information and data, and
- developing information standards.

An example is the NHS Digital guidance on protecting data and handling information securely. The use of public cloud and DSP Toolkit are part of this overall guidance. They are designed to help health and social care organisations to meet the standards required to handle care information.

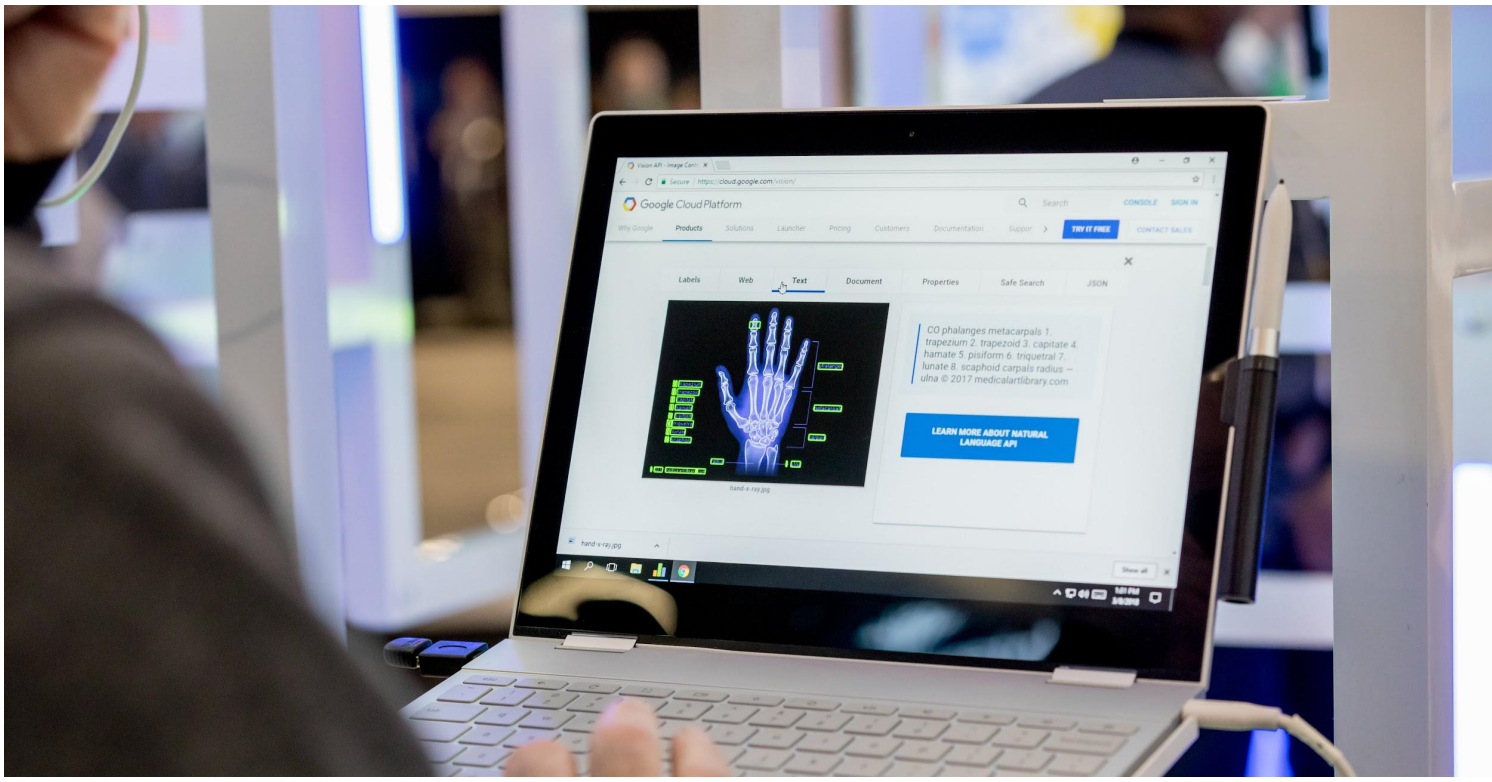
Overview of the Use of Public Cloud Guidance

The UK government introduced a 'Cloud First' policy for the public sector in 2013. This was reassessed in 2019 and remains a flagship policy, see Cloud Guide for the Public Sector 2020.

The future of healthcare: our vision for digital, data and technology in health and care policy 2018, recognised how technology is changing our everyday lives including the ability of genomics to help develop personalised medicines for individuals. It mentions how the state of basic IT and clinical tools in health and care is far behind where it needs to be. The paper sets out a number of guiding and architectural principles to help the sector improve the basics and make use of technology such as AI to help diagnose disease as an example. One of the architectural principles is 'public cloud first'. It acknowledges how the use of public cloud provides a number of advantages out of the box.

This is in line with the guidance published by NHS Digital in 2018 for use of Public Cloud Computing services for NHS data. It includes guidance on where data can reside and for Senior Information Risk Owners (SIROs) to ensure they are satisfied with appropriate security arrangements using Cyber Essentials as a guide working with Data Protection Officers (DPO) and Caldicott Guardians.

NHS Digital guidance includes use of specific controls based on security principles, i.e. for data in transit protection, it recommends TLS 1.2 or above or IPsec/TLS VPN gateway. It requires the cloud provider to utilise strong cryptography as defined by NIST SP 800-57 to encrypt communications. This also helps organisations to select a compliant cloud provider based on the minimum standards. The minimum standards are structured around the National Cyber Security Centre (NCSC) 14 Cloud Security Principles. The recommended approach is based on the risk classification for each security principle. See NHS Digital Cloud Security Good Practice Guide Appendix A for the minimum standards. The NHS Digital Health and Social Care Cloud Risk Framework helps organisations to assess and manage risks around use of public cloud.



Overview of the DSP Toolkit

The DSP Toolkit, developed and maintained by NHS Digital in England, helps organisations self-assess and report on their compliance with a defined set of information governance requirements. There are different sets of requirements depending on the organisation type. However, all organisations assess themselves against the 10 National Data Guardian standards.

All organisations, including “Commercial Third Parties,” that have access to health and social care data in England must use the DSP Toolkit to provide assurances around their information governance practices. A Commercial Third Party is “an organisation external to the NHS, contracting with an NHS establishment to provide non-healthcare goods, services that support the establishment providing care to patients.”[2] Cloud service providers may be considered Commercial Third Parties.

As a cloud service provider, Google provides support services to our customers and processes their data with the highest level of care given to maintaining the security and privacy of customer data. We are committed to meeting the service provider's portion of the responsibilities that we share with customers for satisfying the information governance requirements outlined for Commercial Third Parties. We discuss this shared responsibility in the following section.

[2] Organisation Types: NHS Digital

Google Cloud Platform information governance overview

Information governance, which involves the creation, sharing, and use of information assets whilst minimizing security, privacy, and operational risks, is both important and potentially challenging. Google Cloud Platform offers a range of services that help its customers address these challenges. Foundational to these services is security and the protection of data. Understanding Google's approach to security and data protection is therefore critical to understanding how GCP helps customers to meet their information governance requirements.

Google Cloud Platform's approach to security and data protection

Security is at the core of everything we do; it is embedded in our culture and our IT architecture, and we focus on improving it everyday. This section provides an overview of the organisational and technical controls we use to protect our customers' data.

Security best practice centre

GCP's security best practice centre provides references to various security whitepapers and best practices. The best practices guides provide specific, informed guidance on helping secure GCP deployments and describe recommended configurations, architectures, suggested settings, and other operational advice. It contains deployable security blueprints, including code and templates, that can be used to deploy cloud resources in recommended configurations.

Strong security culture

Security is central to Google's culture. It is embedded in our hiring process, employee training, and company-wide events to raise awareness and drive innovation in security and privacy. To learn more about our security culture, refer to the security culture section in the Google Security Whitepaper.

Our security team

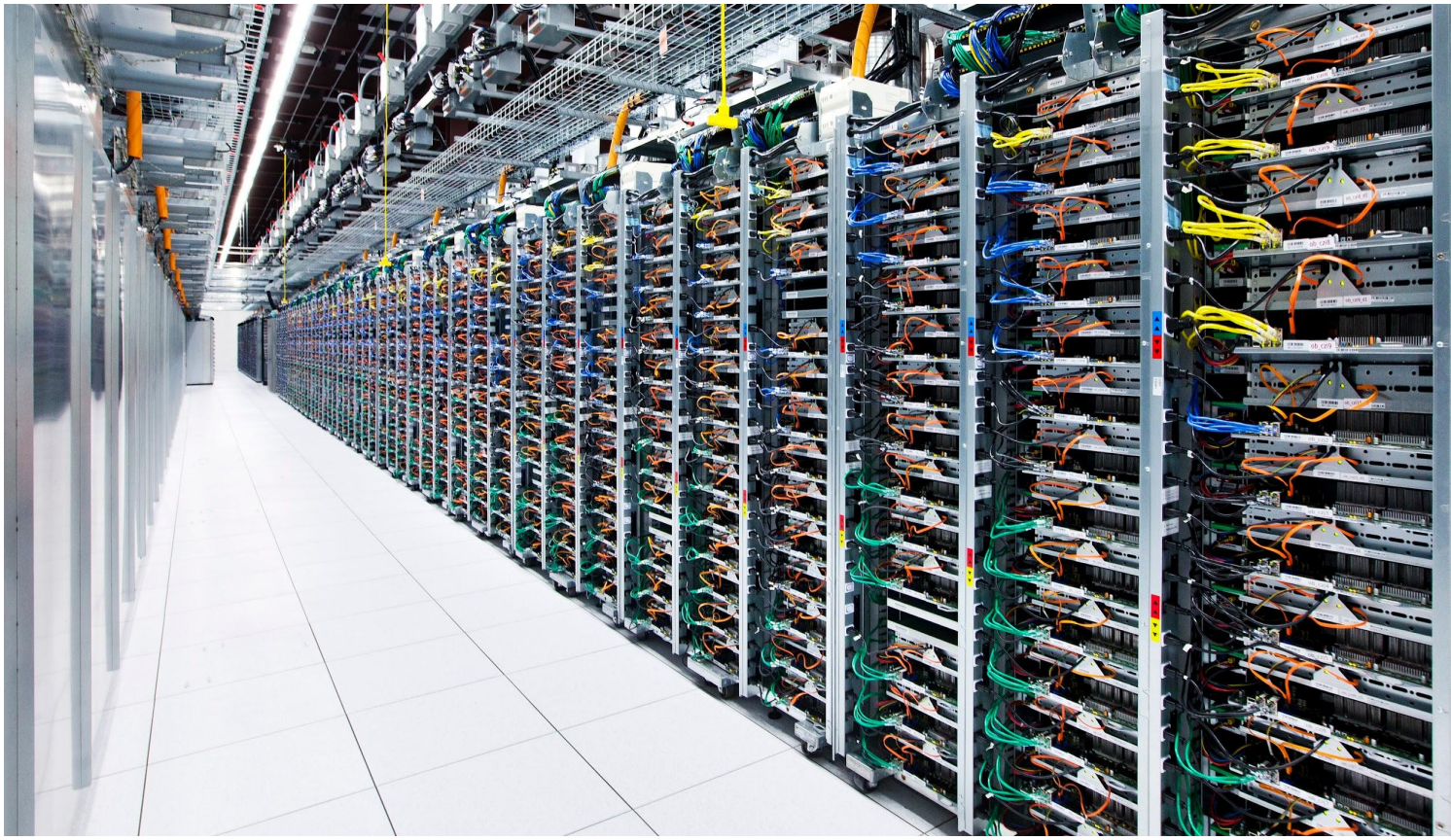
Google employs a global team of security and privacy professionals worldwide, including some of the world's foremost experts. This team maintains the company's defence systems, develops security review processes, builds security infrastructure, implements Google's security policies, and actively scans for security threats. Our team also takes part in research and outreach activities to protect the wider community of Internet users, beyond just those who choose Google solutions. Our research papers are available to the public. As part of our outreach efforts, we have a team known as Project Zero that aims to prevent targeted attacks by reporting bugs to software vendors. To learn more about our dedicated Security and Privacy teams, refer to the Google security whitepaper.

Trusted infrastructure

Google Cloud Platform was conceived, designed and built to operate securely. It runs on the same Google infrastructure that supports multiple of Google's own billion user applications. Google is an innovator in hardware, software, network, and system management technologies. We custom design our servers, proprietary operating system, and geographically distributed data centres. Using the principle of defence in depth, we have created an IT infrastructure that is more secure and easier to manage than most other deployment options, including traditional on-premise technologies. To learn more about our trusted infrastructure, refer to the Google Infrastructure Security Design Overview.

State-of-the-art data centres

Google data centres feature layers of physical security protections. Access to these data centres is limited to only a very small fraction of Google employees. We use multiple physical security controls to protect our data centre floors and we use technologies like biometric identification, metal detection, vehicle barriers, and custom-designed electronic access cards. Our data centres are monitored 24/7/365 to detect and track intruders. Data centres are routinely patrolled by experienced security guards who have undergone rigorous background checks and training. To learn more about our data centres, refer to Google Data Centres.



Technology

We continue to invest heavily in security, both in the design of new features and the development of cutting-edge tools for customers to more securely manage their environments. Some examples are the Cloud Security Command Center for Google Cloud Platform that brings actionable insights to security teams, and VPC Service Controls that help to establish virtual security perimeters for sensitive data. To learn more about our security technologies, refer to our security products and capabilities page.

Our commitments to data protection

Data is critical to organisations and must be kept safe. We want our customers to feel confident that taking advantage of GCP products does not require them to compromise on security or control of their data. We believe that trust is created through transparency, and we want to be open about our commitments and offerings to our customers when it comes to protecting their data in the cloud.

Our Commitments to Protecting the Privacy of Our Customer's Data

- We promptly notify customers if we detect a breach of Google's security that compromises their data. Refer to our privacy commitments in our Cloud Data Processing Addendum.
- We process our customers' data according to their instructions; we enable customers to access their data and take it out whenever they want.
- We inform our customers where our highly available, resilient, and secure data centers are located.
- Customers can depend on Google's independently verified security practices that are certified and validated by third-party auditors.
- We reject government requests to access our customers' data that are invalid and we publish a transparency report for government requests.

To learn more about our commitments to safeguarding customer information, refer to Google Cloud privacy, our dedicated privacy team and our employee Code of Conduct. We also have a detailed whitepaper on Protecting healthcare data on Google Cloud.

Data access and customer control

Customers own their data, not Google; therefore, you decide how your data will be used on Google Cloud Platform. At Google Cloud Platform, we commit to never using your data for any purpose other than those necessary to fulfill our contractual and legal obligations. In addition, we've designed our systems to limit the number of employees that have access to customer data and to actively monitor the activities of those employees. Access to internal support tools is controlled via Access Control Lists (ACLs) and access authorization is enforced at all relevant layers of the system. To learn more, refer to Google's data access restrictions. We take our Google Cloud Trust Principles very seriously and commit to them in our Cloud Data Processing Addendum.

As part of Google's long-term commitment to transparency and user trust, we provide Access Transparency, a feature that enables customers to review logs of actions taken by Google staff when accessing customer data. For products integrated with Access Transparency, customers have the ability to view logs that capture when, how, and why our administrators access customer data (for example, viewing a label on a Google Cloud Platform Compute Engine instance during a support call) .[3] Learn more about Access Transparency for Google Cloud.

Additionally, Google will retain, return, destroy, or delete customer data in accordance with the contract or service level agreements. To learn what happens when customer data is deleted in Google Cloud Platform and how long it takes to complete Google's data deletion process, refer to the Data deletion on Google Cloud whitepaper.

Industry certifications and independent third-party attestations

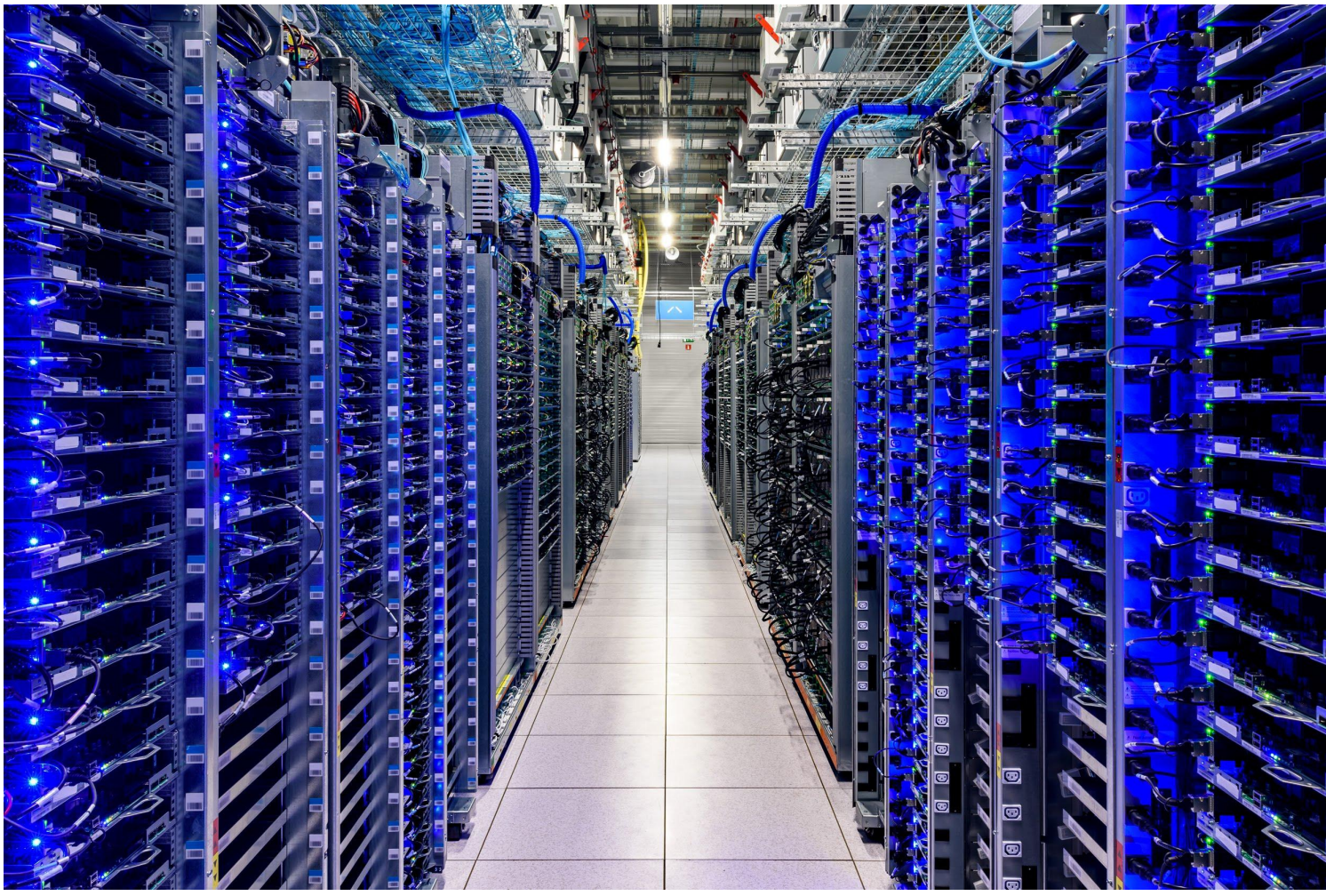
Google Cloud Platform products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn the trust of our customers. We are constantly working to expand our coverage. To learn more about the certifications we have achieved, the laws and regulations we comply with, and the frameworks we align to, refer to our standards, regulations, and certifications page. Customers can self-serve and access our compliance reports directly from the Compliance Reports Manager.

[3] There are some exceptions which are detailed in the Access Transparency documentation.

The Shared Responsibility Model

In the pre-cloud IT model, organisations maintained full responsibility for their environment. They managed everything from the networking and infrastructure to the security controls and applications. In the cloud IT model, management of the IT environment, including responsibilities for security and compliance, is shared between the customer and its cloud service provider. This is often referred to as the Shared Responsibility Model.

Google Cloud Platform's part in the shared responsibility model includes providing services on a highly secure and controlled platform and offering a wide array of security features customers can benefit from. Shared responsibility enables our customers to allocate resources more effectively to their core competencies and concentrate on what they do best. The shared responsibility model does not remove the accountability and risk from customers using Google Cloud Platform services, but it does help relieve the burden as we manage and control system components and physical control of facilities; it also shifts a portion of the cost of security and compliance onto Google Cloud Platform and away from our customers. The different responsibilities held by Google Cloud Platform and its customers are discussed in subsequent sections. For an example of how we define and document roles and responsibilities regarding shared compliance responsibilities, refer to the table in the following sections describing our shared responsibility model for the DSP Toolkit.



How Google Cloud Platform meets NHS Information Governance requirements

The status of our DSP Toolkit compliance can also be found at the NHS site. A full copy of our assessment submission can also be downloaded through the DSP Toolkit site.

The following tables, which are broken into ten sections of data security standards, provide an overview of how Google Cloud Platform meets its information governance requirements for the DSP Toolkit.

Data Security Standard 1

Overview:

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes. Staff understand how to strike the balance between sharing and protecting information, and expertise is on hand to help them make sensible judgments. Staff are trained in the relevant pieces of legislation and periodically reminded of the consequences to patients, their employer and to themselves of mishandling personal confidential data.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
1.1.1	There is senior ownership of data security and protection within the organisation.	Has responsibility for data security been assigned?	Google has established a Code of Conduct training program and requires all employees to complete this training on hire. Management monitors employees' compliance with an online learning system. Google requires all employees, temps, contractors and vendors to abide by Google's policies and procedures, such as the Code of Conduct and Privacy and Information Security Training. Information security is managed by an executive who is dedicated to Security and Privacy, is independent of Information Technology responsibility, and may escalate to the board level concerning security issues.
1.1.2	There is senior ownership of data security and protection within the organisation.	Who are your staff with responsibility for data protection and/or security?	*Google Information Security team*: Google establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, Google assigns responsibilities to the Google Information Security team.

			Google manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of Google products and services.
1.2.1	There are clear data security and protection policies in place and these are understood by staff and available to the public.	Are there approved data security and protection policies in place that follow relevant guidance?	Google has security policies addressing confidentiality, integrity, and availability topics, including those required by DSP Toolkit. These have been approved by management and published on the intranet which is accessible to all employees. This has been tested as a part of Google Cloud Platform's ISO/IEC 27001 certification. Information is available publicly here.
1.2.2	There are clear data security and protection policies in place and these are understood by staff and available to the public.	When were the data security and protection policy or policies last updated?	Security policies are reviewed at least annually. Supporting procedures and guidelines are created/updated as needed. This has been tested as a part of Google Cloud Platform's ISO/IEC 27001 certification.
1.2.3	There are clear data security and protection policies in place and these are understood by staff and available to the public.	How are data security and protection policies available to the public?	The SIRO approves Google security policies on an annual basis. This has been tested as a part of Google Cloud's ISO/IEC 27001 certification. Policies are available here.
1.3.2		How is transparency information (e.g. your Privacy Notice) published and available to the public?	Since GCP operates as a data processor, our customers act as a data controller and therefore, determine the nature of their data processing activities. It is the customers' responsibility to determine how they use the platform and what data they import into it. GCP as a data processor, is responsible for providing tools and functionality that enable its customers. Refer here for more details. Google will only process customer data in accordance with the Cloud Data Processing Addendum, and will not process customer data for any other purpose.
1.3.3		How have Individuals been informed about their rights and how to exercise them?	
1.3.4		Provide details of how access to information requests have been complied with during the last twelve months.	
1.4.1	Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)	Provide details of the record or register that details each use or sharing of personal information.	
1.4.2		Provide a list of all systems/information assets holding or sharing personal information.	
1.4.4		Is your organisation compliant with the national data opt-out policy?	

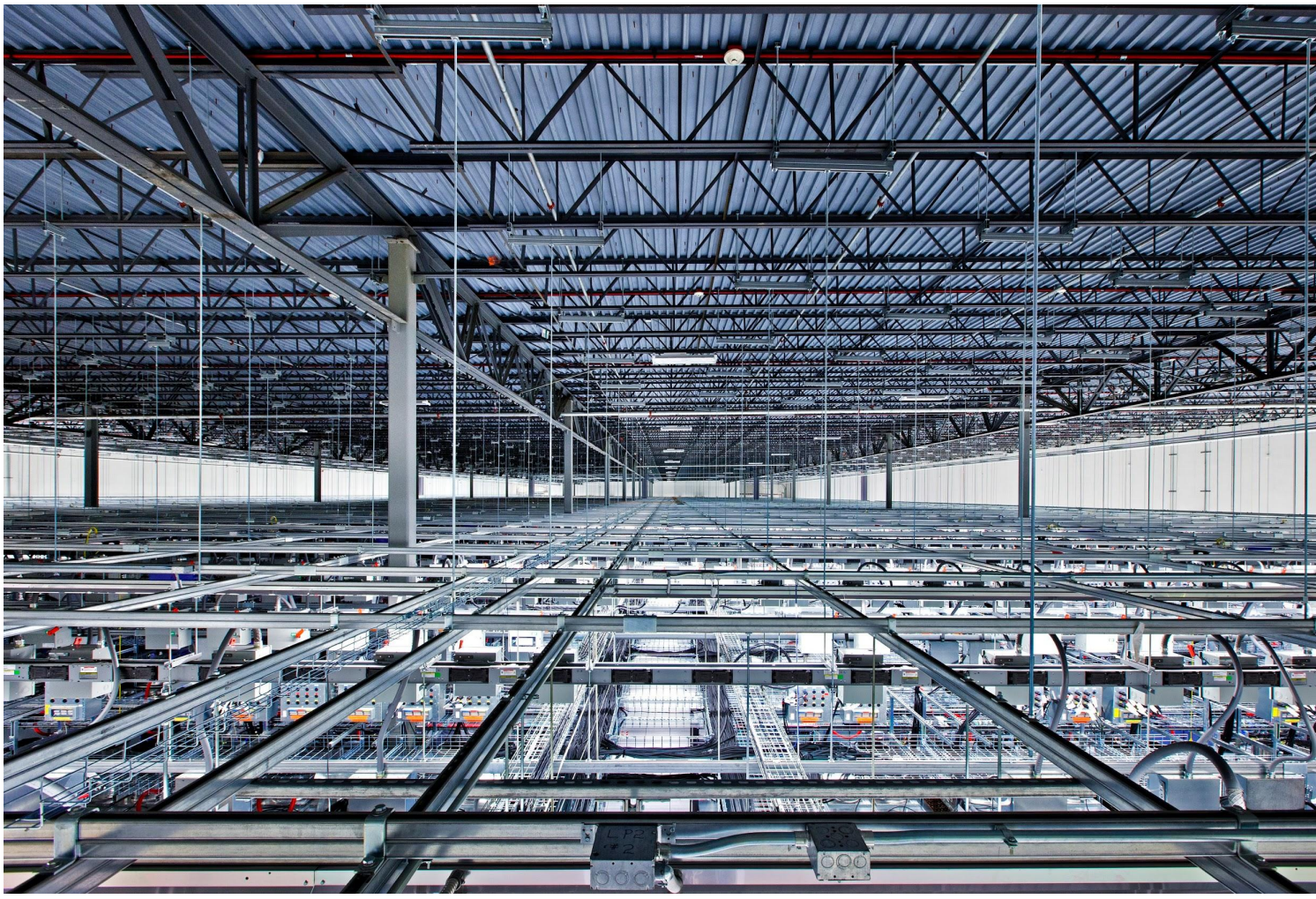
1.5.1	Personal information is used and shared lawfully.	Is there approved staff guidance on confidentiality and data protection issues?	Google has a 'Data Security Policy' to ensure that personal information is being used and shared lawfully. In addition, during orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Google establishes security policies and procedures, which clearly define information security responsibilities for all employees. Within the information security policies and procedures, Google assigns responsibilities to the Google Information Security team. Google manages operational risk by delegating decisions on risk identification and resource prioritization to the various engineering groups that directly support the operation of Google products and services.
1.5.2		What actions have been taken following Confidentiality and Data Protection monitoring/spot checks during the last year?	Google goes through several certifications every year to make sure data protection is spot checked regularly. To know more about Google's current certifications, please refer here. Google has an internal audit function and regularly engages third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.
1.6.1	The use of personal information is subject to data protection by design and by default	There is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.	Google already has processes to build privacy into Google's products from the very earliest stages, and Google is further evolving its practices, including the Cloud Data Processing Addendum , to meet the GDPR's requirements around Privacy by Design and Privacy by Default. Google has issued 'Data Classification Guidelines' that were developed to describe how data is classified at Google and should be handled, including pseudonymized and anonymous information. Google has policies and procedures in place which govern the use and protection of personally identifiable information.
1.6.2		There are technical controls that prevent information from being inappropriately copied or downloaded.	Google has a User Data Access Policy that defines the rules for collecting, accessing, processing, and handling User Data at Google. Google has information security and data access policies and controls in place to prevent unauthorized access, alteration,

			disclosure, or destruction of important records.
1.6.3		There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Google has a Physical Security Policy that describes how people and property is protected at Google. Additionally, Google's focus on security and protection of data is among its primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Google data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As one gets closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever set foot in one of Google's data centers. Physical protection and guidelines are described in the Physical Security Policy, Data Security Policy, Google Photography Policy, and the Data Center Access policy Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, biometric identification mechanisms, and/or physical locks Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems Data center perimeters are defined and secured via physical barriers. Physical access to the Corporate Offices is secured via security personnel, badge readers, security credentials (badges) and/or video cameras.

			Google anticipates physical threats to its data centers and has implemented countermeasures to prevent or limit the impact from these threats. The videos here, and this provide an overview of our countermeasures. Additional resources: a) The Cloud Data Processing Addendum describes the security measures that Google will implement and maintain. b) Google Cloud Security White Paper for details on our data center security. c) Information on Data Center Security.
1.6.5		There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO (Information Commissioner's Office) guidance.	Yes. Google has a well defined process to carry out the Data Protection Impact Assessment that follows relevant ICO.
1.6.6		Is a Data Protection Impact Assessment carried out before high risk processing commences?	Google already has processes to build privacy into Google's products from the very earliest stages, and Google is further evolving it's practices, including Data Protection Impact Assessments, to meet the GDPR's requirements around Privacy by Design and Privacy by Default. Google Cloud Platform is operating as a data processor, and therefore our customers, acting as a data controller, determine the nature of their data processing activities. It is the customers' responsibility to ensure they perform a privacy impact assessment in regards to their data and how they plan on using Google's platform.
1.6.7		Have any unmitigated risks been identified through the Data Protection Impact Assessment process and notified to the ICO?	Google Cloud Platform is operating as a data processor, and therefore our customers, acting as a data controller, determine the nature of their data processing activities. It is the customers' responsibility to ensure they perform a privacy impact assessment in regards to their data and how they plan on using Google's platform. Google (taking into account the nature of the processing and the information available to Google) assists Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

			a) providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation); and b) providing the information contained in the Agreement including these Terms.
1.6.8		Data Protection Impact Assessments are published and available as part of the organisation's transparency materials.	Google Cloud Platform is operating as a data processor, and therefore our customers, acting as a data controller, determine the nature of their data processing activities. It is the customers' responsibility to ensure they perform a privacy impact assessment in regards to their data and how they plan on using Google's platform.
1.7.1	Effective data quality controls are in place and records are maintained appropriately.	There is policy and staff guidance on data quality.	
1.7.4		Has a records retention schedule been produced?	It's the customer's responsibility to create a retention schedule based on business needs with reference to statutory requirements and other guidance for the workloads that they hold on top of Google Cloud. Google has a User Data Retention and Deletion Policy. Google has procedures in place to dispose of confidential information according to Google data retention and deletion policy.
1.7.5		Provide details of when personal data disposal contracts were last reviewed/updated.	N/A, Google disposes of its own data being stored logically and destroys its own hard drives as part of data disposal. Google maintains policies regarding the return, transfer, and disposal of user data and makes these policies available to customers. Google sanitizes information system media prior to disposal, release out of organizational control, or release for reuse.
1.8.3	There is a clear understanding and management of the identified and significant risks to sensitive information and services	What are your top three data security and protection risks?	Confidential. The existence of a risk management program to identify and address data security and protection risks on an ongoing basis is addressed by Google's ISO/IEC 27001 Certification. A formal risk assessment is performed at least annually to determine the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with each risk is determined independently,

			considering each risk category. Google develops and maintains a risk management framework to manage risk to an acceptable level. Risks are mitigated to acceptable levels based on risk criteria, including resolution time frames, which are established, documented and approved by management.



Data Security Standard 2

Overview:

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches. All staff understand what constitutes deliberate, negligent or complacent behaviour and the implications for their employment. They are made aware that their usage of IT systems is logged and attributable to them personally. Insecure behaviours are reported without fear of recrimination and procedures which prompt insecure workarounds are reported, with action taken.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
2.1.1	There is a clear understanding of what Personal Confidential Information is held.	The organization has identified and catalogued personal and sensitive information it holds	Google Cloud Platform is operating as a data processor, and therefore our customers, acting as a data controller, determine the nature of their data processing activities. It is the customers' responsibility to ensure they perform a privacy impact assessment in regards to their data and how they plan on using Google's platform. Google has issued Data Classification Guidelines that were developed to describe how data is classified at Google and should be handled, including pseudonymized and anonymous information.
2.1.2		When was the last review of the list of all systems/information assets holding or sharing personal information?	17/4/2020 (as of time of publication of this document). This is reviewed semi-annually and verified as part of Google's ISO/IEC 27001 Certification.
2.2.1	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	Is there a data protection and security induction in place for all new entrants to the organisation?	All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional training on specific aspects of security may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a

			security newsletter that covers new threats, attack patterns, mitigation techniques and more. Google has established a code of conduct training program and requires all employees to complete this training on hire. Management monitors employees' compliance with an online learning system. Google personnel are required to abide by the Code of Conduct and internal privacy and information security policies. Google has established a privacy and information security training program and requires relevant personnel to complete this training annually.
2.2.2		Do all employment contracts contain data security requirements?	The Google Code of Conduct is one of the ways Google puts it's values into practice. All employees and Board members are expected to know and follow the Code. Failure to do so can result in disciplinary action, including termination of employment. Moreover, while the Code is specifically written for Google employees and Board members, Google contractors, consultants, and others who may be temporarily assigned to perform work or services for Google are also expected to follow the Code in connection with their work for Google. Failure of a Google contractor, consultant, or other covered service provider to follow the Code can result in termination of their relationship with Google. Google's Code of Conduct contains the security requirements that employees are expected to adhere to. Google has established a code of conduct training program and requires all employees to complete this training on hire. Management monitors employees' compliance with an online learning system. Google requires employees to sign the Google Confidentiality and Invention Assignment and Arbitration Agreements. Additionally, Google Employees are required to complete the Google Code of Conduct training which addresses responsibilities and expected behavior with respect to the protection of information.

Data Security Standard 3

Overview:

All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit. All staff complete an annual security module, linked to 'CareCERT Assurance'. The course is followed by a test, which can be re-taken unlimited times but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
3.1.1	There has been an assessment of data security and protection training needs across the organisation.	Has an approved organisation wide data security and protection training needs analysis been completed in the last twelve months?	Addressed by Google's ISO/IEC 27001 Certification.
3.2.1	Staff with specialist roles receive data security and protection training suitable to their role.	Have at least 95% of all staff completed their annual Data Security awareness training in the period 1 April to 31 March?	Confidential. The existence of appropriate training coverage is addressed by Google's ISO/IEC 27001 Certification.
3.3.1	Staff with specialist roles receive data security and protection training suitable to their role.	Provide details of any specialist data security and protection training undertaken.	
3.4.1	Leaders and board members receive suitable data protection and security training.	Have the senior people with responsibility for data security received appropriate data security and protection training?	

Data Security Standard 4

Overview:

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. The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff do not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc).

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
4.1.1	The organisation maintains a current record of staff and their roles.	Confirmation that the organisation maintains a current record of staff and their roles.	Addressed by Google's ISO/IEC 27001 Certification. Formal organizational structures exist and are available to Google employees on the Company's intranet. The intranet provides drilldown functionality for identifying employees in each functional team.
4.1.2		Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Addressed by Google's ISO/IEC 27001 Certification. Google has established policies and procedures that govern access to information systems. Google maintains formal user registration and deregistration procedures for granting and revoking access.
4.2.1	Organization assures good management and maintenance of identity and access control for it's networks and information systems.	Date last audit of user accounts held.	17/4/2020 date of last ISO/IEC 27K series certification, at the time of publication of this document. ISO/IEC 27001 audits the access review controls which are performed on a rolling basis throughout the year against the access groups used to control access to Google Cloud Platform infrastructure. Audit of staff accounts occur throughout the year as part of various risk frameworks Google follows. Google uses a version control system, to manage source code, documentation, release labeling, and other functions. Access to the system must be approved. Access to production machines, support tools, and network devices is managed via access control lists. Modification to access control lists are recorded and approved by administrators. Google plans and coordinates system security-related audits with the relevant stakeholders before conducting such activities in order to reduce the impact on internal and consumer users. Google has an established Internal Audit function which evaluates management's compliance with Google's identity management, source code management and infrastructure controls.
4.3.1	All staff understand that their activities on IT systems will	All system administrators have signed an agreement which	Addressed by Google's ISO/IEC 27001 Certification.

	be monitored and recorded for security purposes.	holds them accountable to the highest standards of use.	
4.3.3		Is an acceptable IT usage banner displayed to all staff when logging in, including a personal accountability reminder?	
4.3.4		List of all systems to which users and administrators have an account, plus the means of monitoring access.	Addressed by Google's ISO/IEC 27001 Certification. Google has established policies and procedures that govern access to information systems.
4.3.5		Have all staff been notified that their system use could be monitored?	Google has established a code of conduct training program and requires all employees to complete this training on hire. Management monitors employees' compliance with an online learning system. Google personnel are required to abide by the Code of Conduct and internal privacy and information security policies. Google's internal Code of Conduct clearly states the use of Google's equipment and facilities.

Data Security Standard 5

Overview:

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. Past security breaches and near misses are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviours are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it's not being done properly.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
5.1.2	Process reviews are held at least once per year, where data security is put at risk and following data security incidents.	Provide a summary of process reviews held after security breaches to identify and manage problem processes.	Addressed by Google's ISO/IEC 27001 Certification. Google has an established incident response policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents. Information security incidents are documented per Google's Incident Response Policy. Information from these events are used to prevent future incidents and can be used as examples for information security training. Security policies are reviewed at least annually. Policies and supporting procedures and guidelines are created/updated as needed. Google has an internal audit function and regularly engages third parties to conduct independent reviews of the effectiveness of the organization's approach to managing information security.

Data Security Standard 6

Overview:

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. All staff are trained in how to report an incident, and appreciation is expressed when incidents are reported. Sitting on an incident, rather than reporting it promptly, faces harsh sanctions. [The Board] understands that it is ultimately accountable for the impact of security incidents, and bears the responsibility for making staff aware of their responsibilities to report upwards. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
6.1.1	A confidential system for reporting security breaches and near misses is in place and actively used.	A data security and protection breach reporting system is in place.	When Google determines there has been a breach, policies and procedures exist to ensure customers are notified in a timely manner in accordance with disclosure laws or contractual agreements. Refer to our Cloud Data Processing Addendum for details. Refer to this whitepaper for details on Google's Data Incident Response process. It is the customer's responsibility as the Data Controller to notify any local bodies such as the UK ICO.
6.1.3		List of all data security breach reports in the last twelve months with action plans.	The list of data security breach reports in the last twelve months is Google Confidential information. Google has a well defined and rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. For information on Incidents and the Google Status Dashboard, refer here. Additionally, Google communicates outage information through its status dashboards: For Cloud Platform: refer here. Google's end-to-end data incident response process is described in this

			whitepaper. Refer to our Cloud Data Processing Addendum for details on data incident policies.
6.1.5		Individuals affected by a breach are appropriately informed.	Addressed by Google's ISO/IEC 27001 audit certification. ***Incident Notification:*** Google has a well defined and rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Additionally, Google communicates outage information through its status dashboards: For Cloud Platform: refer here. Google's end-to-end data incident response process is described in this whitepaper. Refer to our Cloud Data Processing Addendum for details on data incident policies.
6.2.1	All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway.	Name of anti-virus product.	This is Google Confidential information. The existence of appropriate virus/malware countermeasures is addressed by Google's ISO/IEC 27001 Certification. Antivirus, phishing detection, secure coding, and antimalware/antispam tools are in place to protect Google's information assets. Tools are utilized to detect deviations from pre-defined OS configurations on production machines and correct them.
6.2.2		Number of alerts recorded by the AV tool in the last three months.	
6.2.7		Name of spam email filtering product.	Google has proprietary customer in-house tools for spam email filtering. Spam, phishing, and anti-malware protection mechanisms are in place for Google email. Access to Google's messaging systems are protected by transport layer security and require two factor authentication in the form of user ID, password, security key, and/or certificate. Antivirus, phishing detection, secure coding, and antimalware/antispam tools are in place to protect Google's

			information assets. Tools are utilized to detect deviations from pre-defined OS configurations on production machines and correct them.
6.2.9		Number of phishing emails reported by staff per month.	This is Google Confidential Information. Note that Google uses Gmail as our email platform, and Gmail as a platform uses the latest advancements in machine learning and detection algorithms to scan emails, blocking 99.9% of spam and phishing messages. For more information, please refer to these resources: • https://security.googleblog.com/2017/05/protecting-you-against-phishing.html • https://cloud.google.com/blog/products/g-suite/protecting-you-against-phishing • https://cloud.withgoogle.com/security/us/protect-people Spam, phishing, and anti-malware protection mechanisms are in place for Google email. Access to Google's messaging systems are protected by transport layer security and require two factor authentication in the form of user ID, password, security key, and/or certificate.
6.3.1	Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.	If you have had a data security incident, was it caused by a known vulnerability?	There are no known vulnerabilities that are yet to be remediated at this time. Google Cloud Platform is the data processor. Customers of Google Cloud Platform are data controllers. They will have access to CareCERT and will be responsible for acting on any CareCERT advice where appropriate.

Data Security Standard 7

Overview:

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management. A business continuity exercise is run every year as a minimum, with guidance and templates available from [CareCERT Assurance]. Those in key roles will receive dedicated training so as to make judicious use of the available materials, ensuring that planning is modelled around the needs of their own business. There should be a clear focus on enabling senior management to make good decisions, and this requires genuine understanding of the topic, as well as the good use of plain English. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
7.1.1	Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services.	Organisations understand the health and care services they provide.	Google Cloud Platform is operating as a data processor, and therefore our customers acting as a data controller, determine the nature of their data processing activities. It is the customers' responsibility to determine how they use the platform and what data they import into it. Google Cloud Platform as a data processor, is responsible for providing tools and functionality that enable its customers. Refer here for more information.
7.1.2		Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?	Addressed by Google's ISO/IEC 27001 Certification. Google has implemented business continuity measures to maintain the availability of Google's infrastructure and services. Google has implemented a "follow the sun" model for our information security teams, which ensures that operational responsibility handoffs occur on a routine basis. Google conducts disaster recovery (DR) testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the DR exercise develop testing plans and post mortems which document the results and lessons learned from the tests.

7.1.3		You understand the resources and information that will be needed if there is a data security incident and arrangements are in place to make these resources available.	Addressed by Google's ISO/IEC 27001 Certification. Google has a well defined and rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident involves customer data, Google or its partners will inform the customer and support investigative efforts via our support team. Additionally, Google communicates outage information through its status dashboards: For Cloud Platform: refer here. Google's end-to-end data incident response process is described in this whitepaper.
7.2.1	There is an effective annual test of the continuity plan for data security incidents.	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.	Addressed by Google's ISO/IEC 27001 Certification.
7.2.3		Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held.	
7.3.2	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Addressed by Google's ISO/IEC 27001 Certification. Online copies of emergency contacts are kept securely, and are up-to-date.

Data Security Standard 8

Overview:

No unsupported operating systems, software or internet browsers are used within the IT estate. Guidance and support is available from CareCERT Assurance to ensure risk owners understand how to prioritise their vulnerabilities. There is a clear recognition that not all unsupported systems can be upgraded and that financial and other constraints should drive intelligent discussion around priorities. Value for money is of utmost importance, as is the need to understand the risks posed by those systems which cannot be upgraded. It's about demonstrating that analysis has been done and informed decisions were made.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
8.1.1	All software has been surveyed to understand if it is supported and up to date.	What software do you use?	The software is proprietary, maintained by Google. Refer here for the list of Google Cloud Platform products and the underlying infrastructure, that are within the scope of this assessment.
8.2.1	Unsupported software is categorised and documented, and data security risks are identified and managed.	List of unsupported software prioritised according to business risk, with remediation plan against each item.	The vast majority of Google's software underlying the Google Cloud products is Google proprietary, and therefore does not become "unsupported". Google is able to mitigate the risk through a proprietary software stack that it manages any obsolescence within.
8.2.2		The person with overall responsibility for data security confirms that the risks of using unsupported systems are being treated or tolerated.	
8.3.1	Supported systems are kept up-to-date with the latest security patches.	How do your systems receive updates and how often?	Google has Device Configuration Guidelines, that are developed in accordance with our Network and Computer Security Policy and Data Security Policy. Device Configuration Guidelines specify the security requirements for the configuration and management of devices connecting to Google's internal networks.
8.3.2		How often, in days, is automatic patching typically being pushed out to remote endpoints?	End points are continuously patched, as patches become available, which vary depending on OS and applications. Google's Device Configuration Guidelines apply to any device that connects to Google's internal networks or accesses Google's corporate services. Workstations (e.g. desktops, laptops) and servers connected to the network,

			including their critical operating system components like the kernel, are centrally managed and monitored. Updates and security patches are centrally managed and pushed as needed by the Security team.

Data Security Standard 9

Overview:

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. [CareCERT Assurance] assists risk owners in understanding which national frameworks do what, and which components are intended to achieve which outcomes. There is a clear understanding that organisations can tackle the NDG Standards in whichever order they choose, and that the emphasis is on progress from their own starting points.

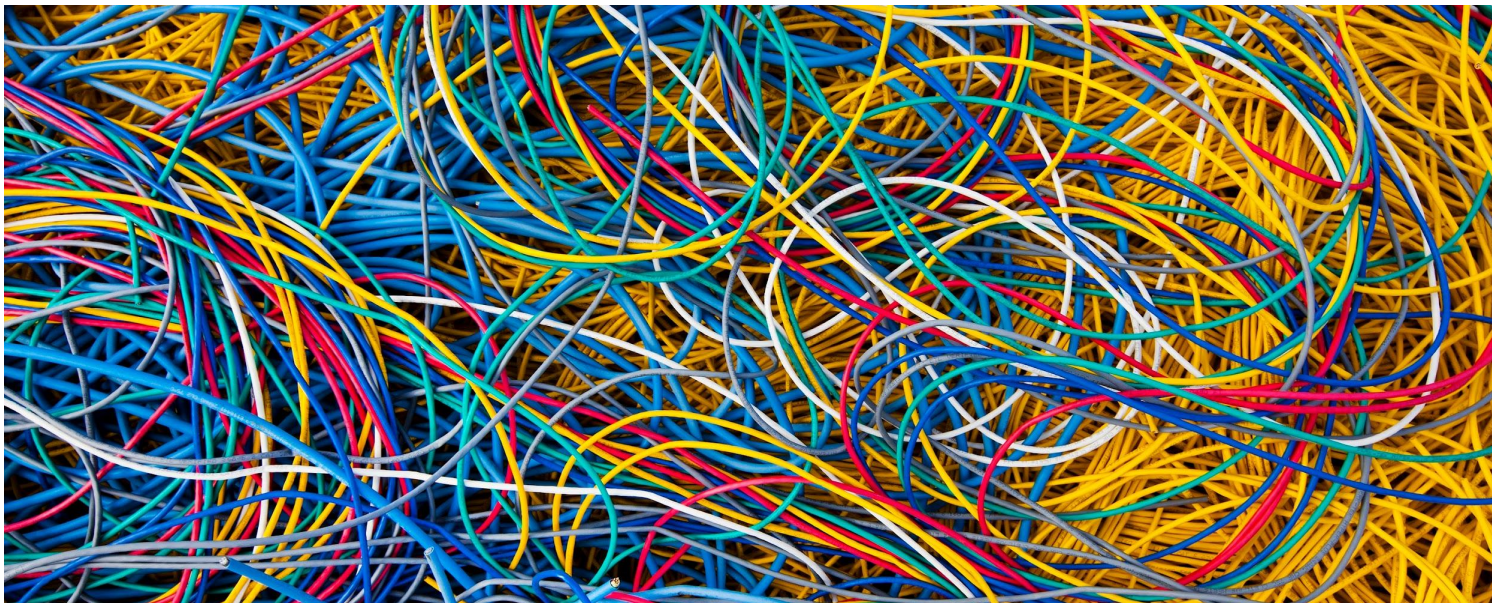
DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
9.1.1	All networking components have had their default passwords changed.	The Head of IT, or equivalent role confirms all networking components have had their default passwords changed.	Addressed by Google's ISO/IEC 27001 Certification. Google has a password change system that enforces Google's password policy.
9.2.1	A penetration test has been scoped and undertaken	The annual IT penetration testing is scoped in negotiation between management, business and testing team including checking that all networking components have had their default passwords changed.	Addressed by Google's ISO/IEC 27001 Certification. Penetration tests are performed at least annually.
9.6.2		Confirm all health and care data is encrypted at rest on all mobile devices and removable media.	Google prohibits the use of removable media for the storage of PII unless the data has been encrypted.

Data Security Standard 10

Overview:

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

DSP Toolkit Req#	Assertion	Requirement	How Google Cloud Platform meets this requirement
10.1.1	The organisation can name its suppliers, the products and services they deliver and the contract durations.	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.	Google maintains a publicly available list of subprocessors and a procedure is in place to disclose changes to the customer before their use. Google has developed policies and procedures that govern third party relationships. Refer to the Cloud Data Processing Addendum for details. Information about the location of Google's facilities and where individual Google Cloud Platform services can be deployed is available here.
10.2.1	Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance.	Organisations ensure that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	Google Cloud Platform is operating as a data processor, and therefore our customers acting as a data controller, determine the nature of their data processing activities. It is the customers' responsibility to determine how they use the platform and what data they import into it. Google Cloud Platform as a data processor, is responsible for providing tools and functionality that enable its customers. Refer here for more information.



How Google Cloud Platform helps customers meet their DSP Toolkit requirements

Our customers are responsible for ensuring they comply with their regulatory obligations including those associated with the DSP Toolkit. Google Cloud Platform helps its customers by providing services on a highly secure and controlled platform and by offering a wide array of security products for customers to choose from that can assist them with meeting regulatory requirements and reducing the technical burden and cost of compliance. The status of our DSP Toolkit compliance can be found here.

Google Cloud Platform products to help with compliance

GCP delivers a range of product offerings to help customers meet compliance requirements. We list some of these products and services in the table below. For a full list, refer here.

Category	Offering	Description
Governance	Cloud Console	Integrated Google Cloud Platform management console
	Cloud Console Mobile App	Manage Google Cloud Platform services from your Android or iOS device
	Cloud Deployment Manager	Create and manage cloud resources with simple templates.
	Cloud Endpoints	Develop, deploy, and manage APIs on any Google Cloud Platform back end.
	Cloud Shell	Manage your infrastructure and applications from the command-line in any browser.
Identity and Access Management	Certificate Authority Service	Simplify the deployment and management of private CAs without managing infrastructure.
	Cloud IAM	Unified platform for IT admins to manage user devices and apps
	Context-aware access	Manage access to apps and infrastructure based on a user's identity and context
	Identity and Access Management	Permissions Management System for Google Cloud Platform resources
	Identity-aware Proxy	Use identity and context to guard access to your applications and VMs.
	Identity Platform	Add Google-grade identity and access management to your apps.
	Managed Service for Microsoft Active Directory	Hardened service running Microsoft Active Directory
	Policy Intelligence	Smart access control for your Google Cloud Platform

		resources
	Resource Manager	Hierarchical management for organizing resources on Google Cloud Platform
	Titan Security Key	Two-factor authentication device for user account protection
Data Security	Cloud Data Loss Prevention	Fully managed service designed to help you discover, classify, and protect your most sensitive data.
	Cloud Key Management	Manage encryption keys on Google Cloud Platform
	Encryption at Rest	Encryption at rest by default, with various key management options
	Encryption in Transit	Default TLS encryption provided to protect data in transit between customers and Google infrastructure
	Secret Manager	Store API keys, passwords, certificates, and other sensitive data.
Network Security	Application Layer Transport Security	Mutual authentication and transport encryption system
	Cloud Firewalls	Global and flexible firewalls to protect your cloud resources
	Cloud Load Balancing	High performance, scalable load balancing on Google Cloud Platform.
	Google Cloud Armor	Help protect your applications and websites against denial of service and web attacks.
	Identity Aware Proxy	Use identity and context to guard access to your applications and VMs.
	Virtual Private Cloud (VPC)	Managed networking functionality for your Google Cloud Platform resources.
	VPC Service Controls	Isolate resources of multi-tenant Google Cloud Platform services to mitigate data exfiltration risks.
Infrastructure Security	Binary Authorization	Deploy only trusted containers on Google Kubernetes Engine
	Confidential Computing	Encrypt data in-use with Confidential VMs. Available in Beta for Google Compute Engine.
	Container Security	Secure your container environment on GCP, GKE, or Anthos.
	Shielded VMs	Hardened virtual machines on Google Cloud Platform.
	Apigee API Management Platform	Design, secure, analyze, and scale APIs anywhere with visibility and control.
	User Protection Services: Phishing Protection	Protect your users from phishing sites

Application Security	User Protection Services: reCAPTCHA Enterprise	Help protect your website from fraudulent activity, spam, and abuse.
	User Protection Services: Web Risk	Detect malicious URLs on your website and in client applications.
Security Monitoring and Operations	Access Transparency	Cloud provider visibility through near real-time logs
	Cloud Asset Inventory	View, monitor, and analyze Google Cloud Platform and Anthos assets across projects and services
	Operations (formerly Stackdriver)	Monitor, troubleshoot, and improve application performance on your Google Cloud Platform environment.
	Security Command Center	A security management and data risk platform that helps with security vulnerabilities and threats.
Compliance	Assured Workloads	Compliance and security controls for sensitive workloads
Security Analytics	Chronicle	Extract signals from your security telemetry to find threats instantly

Google Cloud Platform Terms of Service and Conditions

We provide contractual commitments to help our customers as they continue their compliance journeys.

We encourage healthcare organizations to read the commitments we've made to protecting the privacy of your data and your customers' data, which are detailed in our Google Cloud Trust Principles. We understand that the privacy of your data, as well as your customers' health information and data is of paramount importance to you. In addition to committing to our Google Cloud Trust Principles, we build privacy into our products from the earliest stages, and continually evolve our practices. We articulate those commitments in our Cloud Data Processing Addendum; and undergo regular independent, third-party audits to verify these protections.

Additional Resources to help Google Cloud Platform customers

We provide the following additional resources to help our customers as they continue on their compliance journeys.

Documentation	We share documentation including how-to guides, best practices for enterprises, best practices for security, blog posts, FAQs, and whitepapers like this one to help customers access the information they need at any time.
Audit Logs	Google Cloud Platform services write audit logs that help customers answer the questions of "who did what, where, and when?"
Technical Support Services	We offer different support options including free support resources and access to online communities of Google Cloud Platform enthusiasts, experts, and Google employees to choose from.
Training and Certifications	We offer training and certifications for customers to learn the technical skills and best practices that will help them make the most of GCP product offerings.
Tutorials	We provide tutorials to help customers get started with GCP products and services.
Compliance Resource for Healthcare and Life Sciences	We offer a dedicated section on Compliance Resources for Healthcare and Life Sciences, including a whitepaper on protecting health and social care data on GCP.
Specialised Sales	The Google Cloud UK public sector sales team consists of commercial and technical specialists, part of their role is to help customers with their journey to and on the Cloud.

Conclusion

Organisations that electronically handle UK health and social care data can take advantage of GCP Google Cloud products and services to help meet their information governance requirements. Meeting information governance requirements is easier with a trusted cloud service provider like Google. This whitepaper describes how we have implemented DSP Toolkit requirements and how we can help our customers meet their DSP Toolkit requirements. The information in this whitepaper can also be referenced as customers seek to design, build, and deploy applications on GCP that will handle sensitive information correctly, protecting it from unauthorized access, loss, damage, and destruction.