Global Alliance for Genomics and Health

SECURITY TECHNOLOGY INFRASTRUCTURE

Standards and implementation practices for protecting the privacy and security of shared genomic and clinical data

VERSION 2.0, August 9, 2016

1. Introduction

This document describes the security technology infrastructure recommended for stakeholders (see section 2.1 below) in the *Global Alliance for Genomics and Health* (GA4GH) ecosystem. As a living document, the *Security Technology Infrastructure* will be revised and updated over time, in response to changes in the GA4GH *Privacy and Security Policy*, and as technology and biomedical science continue to advance.

The GA4GH is an unincorporated collaboration among entities and individuals pursuing the common mission of accelerating progress in medicine and human health by advancing a common infrastructure of harmonized approaches to enable effective and responsible sharing of genomic and health-related data. The GA4GH functions as an interdependent, self-regulated ecosystem wherein each entity and individual is responsible for operating and behaving consistently with a set of common values and expectations set forth in the *Framework for Responsible Sharing of Genomic and Health-Related Data*.[1] The viability and success of the GA4GH is directly dependent upon *trust* – the ability of Alliance stakeholders to trust each other, and the ability of individuals who contribute their clinical and genomic data to trust GA4GH stakeholders to use their data responsibly and respectfully.

As an interdependent, emergent ecosystem, the GA4GH supports multiple physical and logical architectures. Therefore, the security technology infrastructure described herein is not intended to describe a physical or operational implementation, but rather suggests a set of security and architectural standards and guidelines for implementing and operating a trustworthy ecosystem. Given the important role that trust plays in pursuing the mission of the GA4GH, the security technology infrastructure is not limited to those mechanisms traditionally considered "security" technologies, such as authentication, authorization, access control, and audit, but also includes architectural guidance for building and operating trustworthy systems – that is, systems that can be relied upon to perform their expected functions and to resist both malicious attack and disruptions.

The *Framework for Responsible Sharing of Genomic and Health-Related Data* describes the principles that form the trust foundation for GA4GH. The *GA4GH Privacy and Security Policy*

[2] builds upon the *Framework* by articulating policies for securing the data and services provided under the auspices of the GA4GH, and the privacy of the individuals who enable their genomic and health-related data to be discovered, accessed, and used. The *Security Technology Infrastructure* defines guidelines, best practices, and standards for building and operating a technology infrastructure that adheres to the GA4GH *Framework* principles and enforces the GA4GH *Privacy and Security Policy*.

The technology infrastructure defined herein seeks to reflect the current state of practice, while enabling emerging approaches to sharing sensitive information on a massive scale. It is intended to support a broad range of existing use cases, while allowing innovation.

We anticipate that many organizations will build upon an existing ISO/IEC 27001:2013 conformant Information Security Management System in order to accomplish compliance with the *GA4GH Security Technology Infrastructure*. Thus we have included content similar to ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls* [3], which recommends information security controls for addressing control objectives arising from identified risks to the confidentiality, integrity, and availability of information.

The *GA4GH Security Technology Infrastructure* includes the following sections:

2.0 – Security Foundation
- 2.1 – Global Alliance Risk Assessment
- 2.2 – Privacy and Security Policy
- 2.3 – Guiding Principles
- 2.4 – Information Security Responsibilities

3.0 – Security Technology Building Blocks
- 3.1 – Identity Management
- 3.2 – Authorization Management
- 3.3 – Access Control
- 3.4 – Privacy Protection
- 3.5 – Audit Logs
- 3.6 – Data Integrity
- 3.7 – Non-repudiation
- 3.8 – Cryptographic Controls
- 3.9 – Communications Security

4.0 – Operational Assurance
- 4.1 – Physical and Environmental Security
- 4.2 – Operations Security
- 4.3 – Service Supplier Assurances
- 4.4 – Information Security Oversight and Accountability
- 4.5 – Compliance

2. Security Foundation

2.1 Risk Assessment

The *GA4GH Security Technology Infrastructure* is based on a balanced approach to risk management that relies on each individual stakeholder to help protect the security, integrity, and trustworthiness of the GA4GH ecosystem. Each stakeholder should assess its individual risk on an on-going basis and assure that its own implemented policies, procedures, and technology protections are appropriate and sufficient for managing the identified risks not only to the enterprise, but to the GA4GH ecosystem.

To be successful, the GA4GH ecosystem needs to effectively manage the following risks identified by the GA4GH Security Working Group [4].

- Breach of confidentiality – unauthorized disclosure of information that an individual or organization wishes to keep confidential.
- Breach of individual privacy and autonomy – access to and use of an individual's genomic or health-related data without the appropriate knowledge or consent of the individual concerned, or for purposes the individual has not authorized.
- Malicious or accidental corruption or destruction of genomic and health-related data
- Disruption in availability of data and services necessary to maintain appropriate access to genomic and health-related data.
- Unethical, illegal, or inappropriate actions that attempt to breach security controls, surreptitiously obtain or derive information in an unauthorized manner, or otherwise undermine the trust fabric of the GA4GH.

2.2 Privacy and Security Policy

The *Privacy and Security Policy* specifically builds upon the *Framework's* Core Element: "Privacy, Data Protection and Confidentiality." The *Security Technology Infrastructure* recommends technical safeguards, standards, and practices to enforce the *Policy* across the technology implementations that together comprise the GA4GH enterprise.

The *Security Technology Infrastructure* recommends technical safeguards, standards and practices for implementing and operating a technology infrastructure that will enable stakeholders to collectively enforce the *Policy* across the technology implementations that together comprise the GA4GH enterprise.

Thus the *Security Technology Infrastructure* is defined to meet the following five control objectives, responsive to the risks identified above.

- *Control Objective 1*: Implement technology safeguards to prevent unauthorized access, use, or disclosure of confidential and private data.
- *Control Objective 2*: Implement technology safeguards to prevent the discovery, access, and use of individuals' genomic and health-related data, and individual identities, other than as authorized by applicable jurisdictional law, institutional policy, and individual consents.
- *Control Objective 3*: Implement technology safeguards to prevent and detect accidental or malicious corruption or destruction of data.
- *Control Objective 4*: Implement technology safeguards to prevent disruption, degradation, and interruption of services enabling access to data.
- *Control Objective 5*: Implement technology safeguards to prevent and detect potential security attacks and misuse of authorized accesses and privileges.

2.3 Guiding Principles

The *Security Technology Infrastructure* is consistent with the *Framework for Responsible Sharing of Genomic and Health-Related Data*, and with the Guiding Principles developed by the Global Alliance Security Working Group, available on the GA4GH web site (genomicsandhealth.org).

2.4 Information Security Responsibilities

As a virtual ecosystem, the GA4GH assigns roles and responsibilities for information security to stakeholders within this ecosystem. From a security and privacy perspective, the principal stakeholders are:

1. Individuals – people who enable their genomic and health-related data to be used and shared within the GA4GH ecosystem
2. Data stewards – entities responsible for assuring the quality and integrity of data content, and for managing the metadata that preserves context and associated business rules, including privacy and security attributes consistent with applicable law, institutional policy, and individual permissions.
3. Data service providers – entities that provide data storage, protection, management, access, query, and transmission services consistent with GA4GH standard application programming interfaces (APIs) and *Privacy and Security Policy*, and optionally ensure that data transmitted or uploaded to other destinations are qualified according to the specifications for both data and metadata constraints and semantics, as appropriate.
4. Application service providers – entities that provide software and other application services, such as web-based or mobile applications, for manipulating and analyzing data.

5. Infrastructure service providers – entities that provide technology resources and technical support for storing, managing, transmitting, and computing electronic data.

6. Service consumers – individuals and entities that use data and application services available to the GA4GH community.

7. Global Alliance – individuals and entities that provide leadership, sustainment, and cohesion for the GA4GH ecosystem.

Consistent with jurisdictional laws and institutional policy, each data steward, service provider, and service consumer should publish the names, contact information, and roles of the individual(s) who have been delegated responsibility for overseeing conformance with the *Security Technology Infrastructure*.

Figure 1 below is a graphical representation of the delegation of responsibilities for implementing and operating in accordance with the GA4GH *Security Technology Infrastructure*. Color coding indicates the responsibilities of the respective stakeholders.

Infrastructure service providers may provide a wide range of services to data and application service providers, including computing, storage, network, and security services. Most commonly, these services will be virtualized across data centers and geographic locations. The applicability of, and responsibility for providing, each of the security functions within the "service provider" block will depend upon the specific services provided, as well as the contractual agreements established between infrastructure service providers and their customers.

The GA4GH leadership expects that in many cases, one organization may behave in more than one stakeholder role. For example, a data steward may also be a data service provider; an infrastructure service provider might also offer application and data services hosted on the infrastructure they support. In such cases, the organization as a whole is responsible for demonstrating control effectiveness for the applicable controls. The expectation is that stakeholders should document the roles and responsibilities as appropriate within that community.

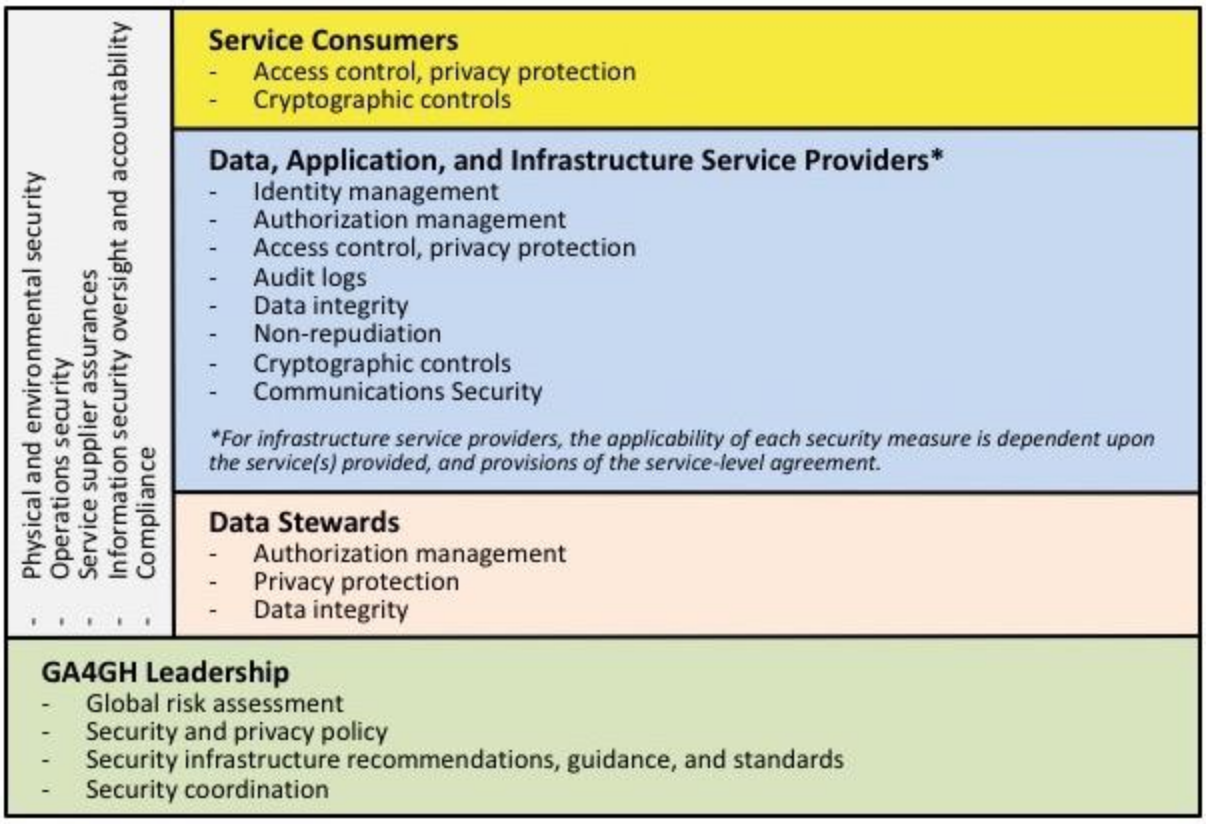

Figure 1. Allocation of responsibility for security protections. Those functions listed in the green block are the responsibilities of the GA4GH community as a whole. Functions in the coral block are performed by data stewards; functions in the blue block are performed by data and application services providers; and functions in the yellow block are performed by consumers of the data and application services offered within the GA4GH community. Functions in the grey block are the responsibility of all service providers, data stewards, and service consumers within the GA4GH ecosystem.

3. Security Technology Building Blocks

This section provides guidance on implementing security services within a stakeholder's organization and across the GA4GH ecosystem. A general principle for building high-assurance infrastructure is to implement security protections as low in the technology stack [23] as possible, given the granularity of control required. To the greatest extent practicable, security features and controls should be implemented at the infrastructure level rather than in applications. For assured protection and greater resistance to tampering and interference, it is preferable to have services such as encryption, access control, auditing, and versioning implemented in the infrastructure than having each application be responsible for them. Integrating security within the infrastructure offers more robust and consistent security protection and compliance, and greatly simplifies application development and testing.

3.1 Identity Management

The effectiveness of the *Security Technology Infrastructure* ultimately is dependent upon the degree to which the actors (individuals and software services) can be trusted to conform to applicable policy.

- Each data and application service exposed within the GA4GH ecosystem will have the capability to electronically authenticate its fully qualified domain name using a server certificate or, within the EU, a qualified electronic signature, as defined in Annex II of Directive 1000/03/EC of the European Parliament and of the Council of 13 December 1999 on a Community infrastructure for electronic signatures.[5]
- Each service provider will authenticate the identity of individuals and software accessing data and services under that provider's control.
- Data and application service providers are encouraged to externalize authentication and authorization to trusted identity providers.
- The level of assurance to which individual identities will be established (i.e., identity proofing) and authenticated will be consistent with the level of risk associated with the actions to be performed by that individual. Suggested levels of assurance are defined in the US National Institute of Standards and Technology (NIST) Special Publication (SP) – 2 [6], as shown in Figure 2 below; each level of assurance comprises a unified set of identity proofing, authentication, and token protection attributes. (Note that NIST SP 800-63-2 is under revision.)
- Service providers may choose to federate authenticated identities and service authorizations using either OASIS Security Assertion Markup Language (SAML) V2.0 [7], or OAuth 2.0 [8] with OpenID Connect [9].

Figure 2. Levels of identity assurance defined in US NIST SP 800-63-2.

Levels of Assurance	Identity Proofing	Identity Authentication	Token Protection
Level 1 (Weak)	None (self- assertion)	Single factor (e.g., password)	Plaintext tokens not passed across network
Level 2 (Moderate)	Presentation of identifying materials or information	Single factor	Cryptographic protection of token during authentication protocol exchange
Level 3 (Strong)	Verification of identifying materials or information	Multi-factor	Cryptographic protection of token during protocol exchange, authentication of verifier; software tokens allowed
Level 4 (Very	In-person verification	Cryptographic	Strong cryptographic, hardware

strong)	of identity	hardware token	token validated at US FIPS 140-2 Level 3 physical security (or

3.2 Authorization Management

- Each data steward is responsible for developing and implementing policies and procedures for determining whether a requesting institutional or individual service consumer is granted access to data sets, and for authorizing rights and privileges associated with that access, in accordance with relevant jurisdictional laws, institutional policies, and data steward authorizations.

- Requests to data stewards for access to data should include, at a minimum: (1) a description of intended uses, consistent with the *Privacy and Security Policy*; (2) assurances that data are being accessed only by authorized individuals; (3) a legitimate and specified time period of access; and (4) a commitment to secure disposal or return of data after use, in accordance with the *Privacy and Security Policy*.

Vetted authorizations issued by trusted third parties may be used as a basis for authorizing service consumers access rights and privileges. For example, a Research Passport issued through the UK National Institute of Health Research (NIHR) Research Passport System [10], may be used as the basis for authorizing researchers access rights and privileges to passport holders. Each service provider should assure that security-critical functions and responsibilities are assigned to multiple roles and multiple individuals in order to avoid conflicts of interest and to prevent inappropriate activities.

Each service provider assigns to each service consumer the minimum access rights and privileges necessary, consistent with the user's identity, affiliation, role, and/or context. Each service provider is responsible for configuring service APIs and service platforms so that they allow access consistent with the *Privacy and Security Policy*, while blocking inappropriate uses and accesses.

Each service provider documents its policies and procedures for adjudicating requests for access to data and services.

3.3 Access Control

- Each service provider and service consumer will implement access controls to assure that only authorized individuals and software may access data and services provided through the GA4GH ecosystem, and that each authenticated user (person or entity) is given access to all of and only those data and services to which it has been authorized.

- Access authorizations may be based on organization, individual user, role, location and context (e.g., purpose, authorization time limits).

- Each service provider and service consumer is responsible for controlling access to genomic and health-related data in accordance with applicable law and the personal authorizations associated with the data.
- Each service provider and service consumer is responsible for assuring that any disclosures of identifiable data include the personal authorization rules the recipient must enforce with respect to access to, and use of, those data.
- Each service provider and service consumer with whom genomic or health-related data are shared will control access to and use of those data in accordance with the personal authorization rules (i.e., consents, permissions) associated with the data

3.4 Privacy Protection

- Each data steward and service provider should use consent-management, access control, usage monitoring, auditing mechanisms, and other privacy-protecting mechanisms dto help ensure that genomic and health-related data are collected, used, shared, and reused only in accordance with the permissions granted by the individual (or authorized representative) to whom the data pertain, and in accordance with jurisdictional law and institutional policies.
- Each data steward should ensure that data coding, de-identification, and anonymization, if used, is performed at the earliest practical point in the workflow to minimize potential exposure of individual identity.
- Each data steward should maintain a data inventory that includes defined sensitivity of data, restrictions on storage and data flows, and contracted data services responsible for enforcing these restrictions.
- Each data steward should monitor data usage to detect attempts to access or use data other than as authorized, including attempts to analytically derive identity.
- Each data steward and data service providers should implement mechanisms to prevent the identity of individuals from being leaked through covert means such as metadata, URLs, message headers, and inference attacks.
- Each data steward is responsible for obtaining the individual authorizations (e.g., consents) required by applicable law and institutional policy, and for conveying these authorizations, or a link to these authorizations, along with the associated data.
- The User Managed Access (UMA) profile [11] of the OAuth 2.0 [12] authorization protocol may be useful in mediating access based on user permissions.
- Each data steward is responsible for updating provenance and confidentiality metadata associated with the data under its control, using HL7 FHIR provenance[13] and confidentiality[14] codes.

3.5 Audit Logs

- Each service provider is responsible for recording and maintaining a log of security-relevant events involving access to or use of resources, data, and services under that entity's control.
- For each security-relevant event, the service provider should record the following data elements:[15] user identification, type of event, date and time, success or failure indication, origination of event, name of affected data, system component, or resource.
- Each service provider should retain the audit log history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up) [15]. This best practice should be interpreted within the constraints of applicable jurisdictional law.
- Each service provider is responsible for monitoring activities on the systems under its control to detect potential security breaches and data misuse.
- Service providers' audit log records should be integratable with existing enterprise security monitoring tools.
- Data stewards and their service providers are jointly responsible for implementing the capability to generate an accounting of accesses to and disclosures of data that can be individually identified or associated with the individual.

3.6 Data Integrity

- Each service provider is responsible for protecting the integrity of genomic and health-related data that it holds, uses, or transmits.
- Each service provider that transmits or receives transmissions containing genomic or health-related data will generate a IETF SHA-2 hash function [16] to verify the integrity of the transmission.
- Each service provider who offers software will assure that it is free from malicious code prior to making it available for distribution.
- Each data steward is responsible for ensuring the accuracy and verifiability of data and associated metadata.
- Each data steward is responsible for assuring that data provenance information is associated with data made available to service consumers.

3.7 Non-repudiation

- Each service provider will have the capability to digitally sign content using a qualified electronic signature, as defined in Directive 1000/03/EC of the European Parliament and

of the Council of 13 December 1999 on a Community infrastructure for electronic signatures [5].

- GA4GH participants who offer downloadable software will digitally sign the downloadable files using a qualified electronic signature, as defined in Annex II of Directive 1000/03/EC of the European Parliament and of the Council of 13 December 1999 on a Community infrastructure for electronic signatures [5].

3.8 Cryptographic Controls

- Each stakeholder will assure that the cryptographic controls used are compliant with all relevant agreements, laws, and regulations.
- Each stakeholder that stores genomic or health-related data will use strong encryption to encrypt the data for storage.
- Each stakeholder will assure that plaintext data encryption keys are not stored in the same system as the data encrypted with those keys. When a key hierarchy is used, plaintext key encryption keys should be stored separately from the system storing data encryption keys.
- Each service provider will use end-to-end transport-level encryption (see section 4.9) to encrypt and integrity-protect data during transmission.

3.9 Communications Security

- Each service provider will assure that communication channels are secured commensurate with the level of risk associated with the content being transmitted.
- Each service provider that transmits genomic or health-related data, or otherwise confidential information, will protect the transport using either the IPsec [18, 19] or Transport Layer Security (TLS) protocol [20].
- Any electronic mail containing genomic, health-related, or other sensitive data will be secured using S/MIME Version 2 [21, 22].

4. Operational Assurance

4.1 Physical and Environmental Security

- Each stakeholder who stores or processes genomic or health-related data is responsible for providing physical safeguards to protect those data in accordance with applicable laws and regulations, institutional policies, and individual consents.
- Each stakeholder who uses a third party to store or process genomic or health-related data is responsible for assuring that business agreements include an obligation to provide physical and environmental data protection.

4.2 Operations Security

- Each data service provider is responsible for assuring that data are stored and protected in compliance with all applicable legal and ethical requirements of the jurisdiction within which the data are stored.

- At the request of an individual whose data are being stored and shared within the GA4GH ecosystem, the responsible data steward should provide the individual information about how their data are being used and for what purposes, as practicable.

- Each data steward will document the privacy and security practices and procedures it uses to make its data and services available within the GA4GH ecosystem, consistent with *Privacy and Security Policy*, and will assure that its service providers make this documentation conveniently available to service consumers and to individuals who contribute their data.

- Each data steward will document the behavioral standards associated with use of the data made available to service consumers, consistent with GA4GH *Privacy and Security Policy*, and will require service consumers to attest to their understanding of, and commitment to adhere to these standards.

- Each service provider will implement privacy and security technology to support adherence to the Fair Information Practices Principles, as articulated in Part Two of the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [17].

- Each service provider will document and enforce written operational procedures for protecting the confidentiality and integrity of data, the availability of services, and the privacy of individuals who contribute their personal data.

4.3 Service Supplier Assurances

Entities that offer data and application services within the GA4GH ecosystem are encouraged to implement architectural assurances that their services can be relied upon to perform their functions as advertised, while resisting malicious attack, adapting to changes, continuing to operate through unanticipated disruptions, and recovering from interruptions and outages. Architectural safeguards include design principles that contribute to the trustworthiness of systems and networks, including but not limited to ability of a system or network to protect the confidentiality and integrity of genomic and health-related data, the availability of data and services, and the privacy of individuals whose data are shared.

All data, application, and infrastructure service providers to the GA4GH community are responsible for implementing appropriate architectural assurances that will enable them to provide a high level of service expectations, as described in each service provider's service level agreement (SLAs). These expectations include:

- Availability – the ability of the service to perform its functions over a specified period of time, generally expressed as the proportion of time that a service is actually available

within an agreed-upon time period. Availability is assured through architectural and design features, and operational procedures that enhance reliability, maintainability, serviceability, and security.

- Scalability (or elasticity) – genomic and health-related data stores should be capable of expanding as the volume of data continues to grow, while protecting the confidentiality, integrity, and availability of data and application services.

- Infrastructure security – security features and processes provided as part of the data or application service offering GA4GH service providers and user organizations should assure that their infrastructure, operating systems, and database management systems isolate applications and datasets to prevent interference from other processes and side-channel attacks. A "least privileges" approach should be used to harden execution environments.

Data stewards should assure that their service suppliers offer the levels of availability, scalability, and infrastructure security necessary to protect the data entrusted to them. Similarly, service consumers should assure that data and application services they use are trustworthy.

4.11 Information Security Oversight and Accountability

- Each stakeholder will document its procedures for responding to potential security incidents.

- Each stakeholder will investigate and resolve security incidents and reported threats as quickly as possible so as to minimize potential disruption of data and application services.

- Each stakeholder will report breaches resulting in the potential disclosure of unencrypted genomic or health-related data, as required by jurisdictional law and regulations, and institutional policy.

- Each service provider who experiences or suspects a data breach involving the potential disclosure of identifiable data is responsible for expeditiously reporting the breach to the data steward responsible for the breached data.

- Each service consumer who experiences or suspects a data breach involving the potential disclosure of identifiable data is responsible for expeditiously reporting the breach to the relevant institutional supervisory authority and to the data steward.

- Each data steward who experiences, suspects, or receives a report of a data breach involving the potential disclosure of identifiable data is responsible for expeditiously reporting the breach to the individuals whose data were breached.

- Each data steward should work with its service providers to assess risks associated with the storage, use, and transmission of genomic and health-related data, and should contractually require appropriate technical mechanisms and procedures for preventing, detecting, and recovering from data breaches, consistent with the assessed risks.

4.5 Compliance

- Each stakeholder is individually responsible for implementing protections consistent with this infrastructure, and for assuring that contracts with third parties address the business partners' obligations to implement such protections.
- Each stakeholder will implement appropriate security procedures to ensure compliance with applicable legislative, regulatory, and contractual requirements relating to the use of genomic or health-related data, and personal information.
- Each stakeholder will implement appropriate security procedures to ensure compliance with applicable legislative, regulatory, and contractual requirements relating to intellectual property rights.
- Each stakeholder is responsible for implementing, and attesting to having implemented, security and privacy processes, procedures, and technology to enforce compliance with relevant legislation, regulations, contractual clauses, and the *Framework for Responsible Sharing of Genomic and Health-Related Data*.
- Each stakeholder will protect audit-log files, business agreements, and other records relating to the stakeholder's participation in the GA4GH ecosystem, from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business agreements.
- GA4GH stakeholders may individually or collectively engage third parties to assess compliance with the GA4GH *Security Technology Infrastructure*, and to evaluate the effectiveness of implemented protections.

5. Definitions

Term	Definition
Access control	Services that assure that users and entities are able to access all of and only the resources (e.g., computers, networks, applications, services, data files, information) that they are authorized to use, and only within the constraints of the authorization.
Audit controls	The collection and recording of information about security- relevant events within a system.
Authentication (person & entity)	Presentation of credentials as proof that the identity asserted by a person or entity attempting to access a system is the identity to which access authorization has been granted. (See "identity management")

Availability	State of a system or network in which it is functioning such that its services and data are available and usable.
Data integrity	Measures to prevent and detect the unauthorized modification and destruction of electronic data during storage and transmission.
Encryption	The process of obfuscating information by running the data representing that information through an algorithm (sometimes called a “cipher”) to make it unreadable until the data are decrypted by someone possessing the proper encryption “key.” Encryption is used for multiple purposes, including the protection of confidential data (at rest and in motion), assurance of data integrity, private communications, and non-repudiation (digital signature).
Identity federation	A usability feature that enables single-sign-on functionality across multiple systems governed under different identity management systems; identity federation is accomplished through agreement among multiple enterprises to accept authenticated identities passed among them as “security assertions.”
Identity management	The total set of administrative functions involved in positively identifying individuals prior to defining them as a known user of a system (i.e., “identity proofing”); issuing access credentials to that identity (e.g., user name and password or other personal identity verification); authorizing and assigning rights and privileges to that identity; and revoking access and privileges when they are no longer needed.
Interoperability	Ability of systems and system components to work together.
Malicious-software protection	Methods to prevent, detect, and remove malicious software (“malware”), which includes any software designed to infiltrate a system without the user’s permission, with the intent to damage or disrupt operations, or to use resources to which the miscreant is not authorized access.
Non-repudiation	Assurance that an actor is unable to deny having taken an action; typically, assurance that a person involved in an electronic communication cannot deny the authenticity of his or her signature on a transmitted message or document.
Privacy risk	Probability that genomic or health-related data will be collected, used, or disclosed in ways that are unauthorized by the individual to whom the data pertain.
Process Isolation	The extent to which processes running on the same system at different trust levels, virtual machines (VMs) running on the same hardware, or applications running on the same computer or tablet are kept separate.
Reliability	Ability of a system, component, or network to perform its specified functions consistently, over a specified period of time
Safety	Property of systems and components that enables them to operate safely,

	or to fail in such a way that no humans are physically harmed as a result.
Scalability	Ability of a system, network, or process to handle a growing amount of work in a capable manner, or its ability to be enlarged to accommodate that growth.
Security risk	Probability that a threat will exploit a vulnerability to expose confidential information, corrupt or destroy data, or interrupt or deny essential information services.
Simplicity	Property of a system or network in which complexity is minimized.
Single sign-on	A usability feature that enables a user to authenticate herself once and then access multiple applications, databases, or systems for which she is authorized, without having to re-authenticate herself.
Transmission security	Protection of electronic data against unauthorized disclosure and modification while the data are being transmitted over a vulnerable network, such as the Internet.

6. References

[1] Global Alliance for Genomics and Health. *Framework for Responsible Sharing of Genomic and Health-Related Data*. 10 September 2014. Available from https://genomicsandhealth.org/about-the-global-alliance/key-documents/framework-responsible-sharing-genomic-and-health-related-data (accessed 5/5/16).

[2] Global Alliance for Genomics and Health. *Privacy and Security Policy*. 26 May 2015. Available from https://genomicsandhealth.org/work-products-demonstration-projects/privacy-and-security-policy (accessed 5/5/16).

[3] ISO/IEC 27002. *Information technology — Security techniques — Code of practice for information security controls*. Available from http://www.iso27001security.com/html/27002.html#Contents (accessed 23 June 2014)

[4] From March 2014 meeting of Global Alliance Security Working Group.

[5]Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures. pp. 0012. Annex II. Available from http://www.mnb.hu/Root/Dokumentumtar/MNB/Kiadvanyok/mnbhu_egyebkiadvanyok_hu/mnbhu_penzstab_fizforg/mnbhu_penzforg_eu/electronic_signature_dir_1999_93_EXTRA.pdf (Accessed 07 July 2014).

[6] US National Institute of Standards and Technology. Electronic authentication guideline. NIST SP 800-63-2. August 2013. Available from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf (Accessed 27 February 2015).

[7] OASIS. Conformance requirements for the OASIS Security Assertion Markup Language (SAML) V2.0. 15 March 2005. Available from http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf. (Accessed 08 July 2014).

[8] OAuth 2.0. Available from http://oauth.net/2/ (Accessed 08 July 2014).
[9] OpenID Connect. Available from http://openid.net/connect/ (Accessed 08 July 2014).

[10] UK National Institute of Health Research. The research passport and streamlined human resources arrangements. Available from http://www.nihr.ac.uk/systems/Pages/systems_research_passports.aspx (Accessed 08 July 2014).

[11] Hardjona, T, Ed. User Managed Access (UMA) profile of OAuth 2.0. Kantara Initiative. 28 Dec 2015. Available from http://docs.kantarainitiative.org/uma/draft-uma-core.html (Accessed 06 May 2016).

[12] The OAuth 2.0 specification is available at http://oauth.net/2/ (Accessed 05 Sept 2014).

[13] Health Level Seven. Resource provenance – Content. Available from

http://www.hl7.org/implement/standards/fhir/provenance.html (Accessed 17 July 2014).

[14] Health Level Seven. HL7 v3 Code System Confidentiality. Available from

http://hl7.org/implement/standards/fhir/v3/Confidentiality/ (Accessed 17 July 2014).

[15] Payment Card Industry Security Standards Council. paragraph 10.3, pp. 55-56

[16] Internet Engineering Task Force. IETF Request for Comment (RFC) 6668. SHA-2 data integrity verification for the secure shell (SSH) transport layer protocol. Available from http://tools.ietf.org/html/rfc6668 (Accessed 08 July 2014).

[17] Organisation for Economic Development and Cooperation. OECD Guidelines on the protection of privacy and transborder flows of personal data. 11 July 2013. pp. 14-15. Available from http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (Accessed 09 July 2014).

[18] Internet Engineering Task Force. Security architecture for the internet protocol. RFC 4301. December 2005. Available from http://tools.ietf.org/html/rfc4301 (Accessed 09 July 2014).

[19] Internet Engineering Task Force. Using advanced encryption standard (AES) CCM mode with IPsec encapsulating security payload (ESP). RFC 4309. December 2005. Available from http://tools.ietf.org/html/rfc4309 (Accessed 09 July 2014).

[20] Internet Engineering Task Force. The transport layer security protocol, Version 1.2. RFC 5246. August 2008. Available from http://tools.ietf.org/html/rfc5246 (Accessed 09 July 2014).

[21] Internet Engineering Task Force. S/MIME Version 2 message specification. RFC 2311. March 1998. Available from http://tools.ietf.org/html/rfc2311 (Accessed 09 July 2014).

[22] Internet Engineering Task Force. S/MIME Version 2 certificate handling. RFC 2312. Available from http://www.ietf.org/rfc/rfc2312.txt (Accessed 09 July 2014).

[23] ISO/IEC 7498-1. Second edition. Information technology – open systems interconnection – Basic reference model. Available from http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip (Accessed 27 February 2015).