SevenBridges

COMPLIANCE WHITE PAPER

COMPLIANCE WHITE PAPER

This white paper describes how the Seven Bridges Platform enables our clients to be compliant with the regulatory frameworks that govern their work and how it keeps their data both private and secure.

TABLE OF CONTENTS

INTRODUCTION

We begin with an overview of the Seven Bridges approach to privacy and security along with a description of the protections built into the Seven Bridges Platform. We then describe how the Seven Bridges Platform enables our clients to stay compliant with standards relevant to performing Next Generation Sequencing in the cloud. In particular, we first provide an overview of HIPAA regulations, which protect patient privacy in the United States, as well as the EU Data Protection Directive program, which govern personal data collected from EU Member States and transmitted to the United States. We next discuss dbGaP Security Best Practices, which lay out requirements that must be met by researchers making use of controlled-access datasets maintained by the NIH, before moving to a discussion of CLIA and CAP policies for researchers interested in clinical applications.

SECURITY STANDARDS AT A GLANCE

STANDARD	COMPLIANCE ON SEVEN BRIDGES PLATFORM	RELEVANT FOR...	BRIEF DESCRIPTION
HIPAA regulations	✔	Healthcare plans, clearinghouses, and providers, and anyone processing patient data on their behalf	Comprehensive but high-level administrative and technical security standards; substantive rules governing use and disclosure of patient data
ISO/IEC 27001:2013	✔	All organizations (international standard for information security risk management).	ISO/IEC 27001:2013 is an international standard, mandating a risk-based approach to information security, verified by rigorous third-party audits
EU General Data Protection Regulation, EU-U.S.Privacy Shield	✔	Organizations based in or collecting personal data from the EU	Substantive rules governing the ways in which personal data may be collected and used
dbGaP Security Best Practices	✔	Researchers making use of controlled-access dbGaP data	Security standards aimed specifically at bioinformatics researchers, including best practices for working in the cloud
CLIA and CAP	✔	Clinical labs	Quality standards aimed at ensuring consistent accuracy, reliability, and timeliness of laboratory testing
FDA (21 CFR Part 11, Quality System Regulation)	✔	Clinical applications	Requirements for data submitted to the U.S. Food and Drug Administration (FDA)

I. PRIVACY AND SECURITY ON THE SEVEN BRIDGES PLATFORM

THE SEVEN BRIDGES SECURITY FRAMEWORK

At Seven Bridges, we believe that it's our job to provide users with end-to-end security and control over their data and analysis so that they can focus on work rather than dealing with complex setups, compliance headaches, and security. To achieve this, we have designed a comprehensive security framework for processing genomic data in the cloud that covers three main areas:

1) **DATA SECURITY:** Ensuring that all sensitive data is kept safe during its full lifecycle. This includes data encryption and secure user authentication.
2) **PLATFORM AND INFRASTRUCTURE SECURITY:** Ensuring that the software platform and its underlying infrastructure (server and network) support the secure architecture.
3) **SECURITY CONTROLS:** Ensuring security of the system by implementing administrative, technical, and other security controls, while at the same time ensuring compatibility with a broad range of trusted information security frameworks and compliance requirements.

The following three sections present Seven Bridges' take on each of these three areas and provide concrete implementation examples from the Seven Bridges cloud platform. Since the cloud version of the Seven Bridges Platform is built on pre-existing cloud infrastructure, such as that provided by Amazon Web Services (AWS) and Google Cloud Platform, we use provider terminology for the remainder of this paper, such as storage buckets and computation instances.

Please refer to https://aws.amazon.com/ or https://cloud.google.com/ for details.

DATA SECURITY

The key security consideration for data of any kind is whether it is safely contained and isolated. Only an authorized user should be able to access or copy it. This not only means that data needs to be encrypted at all times, but also that tight controls need to be implemented around authentication and encryption key storage. In addition, certain laws and regulations specifically require control over data locality (where, geographically, data can be stored and transferred).

A phrase that is often heard in regard to encrypting genomic data is that it must be "encrypted during transfer and at rest." While encryption during transfer is fairly straightforward from an implementation standpoint (the scheme used by Seven Bridges is outlined below), encryption "at rest" is not uniquely defined. Using a cloud environment such as AWS or Google Cloud Platform, there are actually two different types of "at rest" storage: permanent storage on cloud storage (such as AWS S3 or Google Cloud

Storage), and ephemeral storage used by the computation instances.

AT REST

The Seven Bridges Platform implements both types of "at rest" encryption. Data is by default uploaded only to encrypted objects leveraging server-side encryption, both on AWS S3 or Google Cloud Storage. During computation, all disk volumes used for ephemeral storage are encrypted using an industry standard AES-256 cipher. The Platform can also support integration with various methods of encryption key management for volume encryption/decryption, such as AWS KMS, depending on what level of security and privacy is needed.

IN TRANSIT

During data transfers, all user data is transferred exclusively through encrypted TLS/SSL channels throughout, for all data flows shown in Figure 1.

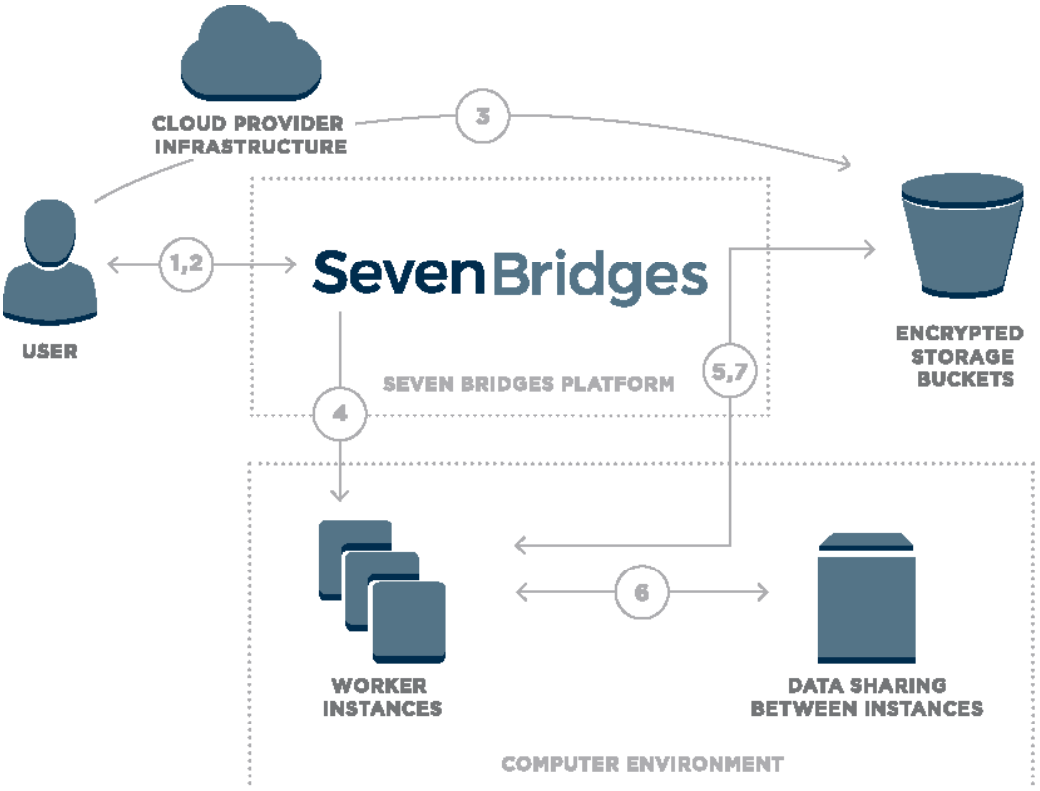

Figure 1 - Overview of data flow on the Seven Bridges Platform

1) User logs onto the platform
2) Platform creates a unique signed URL for the user
3) Using signed URL, data is uploaded to an encrypted storage bucket
4) Once the user starts a compution, the Seven Bridges platform calculates the optimal execution plan and starts up task worker instances
5) Worker instances securely pull data from cloud storage
6) Worker instances are able to securely share intermediate data
7) Final results are uploaded to cloud storage

At the end of the data lifecycle, a strict data purging policy ensures that all data is safely

deleted if it is no longer needed on ephemeral storage or when an authorized user chooses to delete data on the platform.

AUTHORIZATION AND ACCESS CONTROLS

While encryption and the safe purging of ephemeral data are key to protect it in the cloud, they are only effective with appropriate authorization and access controls. Access controls on the Seven Bridges Platform have been implemented in a very fine-grained manner. Rather than establishing principal "file owners," access permissions are set on a per-user-per-project basis, meaning that a user's access permissions to a given file can depend on the context (project) in which this file is being used. This includes sharing of data, which can only be performed via the platform itself unless users have the explicitly granted permissions to download a file. Seven Bridges retains audit logs for all data access for six years to ensure regulatory compliance (as required by HIPAA).

By default, users authenticate on the platform through a username and secure password, however single sign-on via SAML2 protocol is supported out of the box. The Seven Bridges Platform can also support more strict data access control with client-encryption, two-factor authentication, and integration of external key management.

PLATFORM & INFRASTRUCTURE SECURITY

Running the Seven Bridges Platform on industry-leading cloud infrastructure providers allows us to take advantage of the broad spectrum of built-in compliance *(see https://aws.amazon.com/compliance/ and https://cloud.google.com/security/compliance)* and security *(see https://aws.amazon.com/security/ and https://cloud.google.com/security)* features provided by the underlying infrastructure. These features include physical datacenter security and network infrastructure security to secure media handling and data encryption. Naturally, compliance of the cloud provider does not imply compliance of the overall platform and ecosystem, but it is a solid foundation on which to build.

In addition, Seven Bridges secures its infrastructure in a number of ways:

1) All AWS computation instances run within Virtual Private Clouds (VPC). VPCs are logically isolated networks within the AWS cloud and kept only minimally open for the necessary external and internal access.
2) All Google Cloud (GCE) computation instances run on separate networks, similar in functionality to AWS VPC with similar firewall configuration, allowing only necessary services for external and internal access.
3) Users can choose to isolate all computation resources through an "Instance Lockdown" mode that disables any access to the project data or computational instance during the computation, even by platform admin staff.
4) Best security practices regarding tenancy, such as AWS Architecting for HIPAA are followed.
5) Computation **instance reuse is limited** to the same user and project to prevent data leakage.
6) Bioinformatics apps run within **LXC containers** managed by Docker software with restricted Linux capabilities and strict firewall implemented.

Access to the production and development environments are secured through Virtual Private Networks as shown in Figure 2.

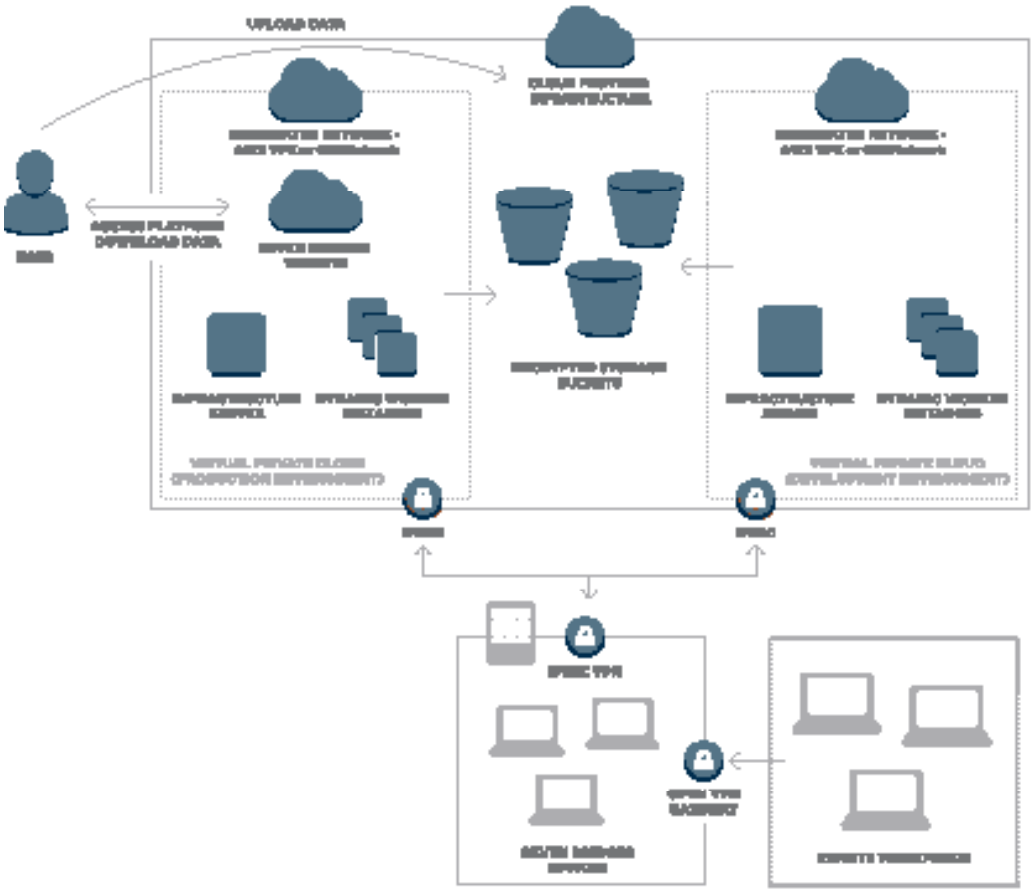

Figure 2 - Overview of network security on the Seven Bridges Platform

In addition to building on a secure foundation, we also we constantly monitor and improve the Seven Bridges Platform by following best-practices *(including SANS Top-20)* of infrastructure stability and security, including:

1) Monthly software and infrastructure vulnerability assessments to discover vulnerabilities and remediate them.

2) Regular penetration tests to discover vulnerabilities in the system which may not be noticed in a regular vulnerability assessment.

3) Regular audit log analysis and system-level inspection to look for suspicious behavior, potential attacks, and security breaches.

4) A strict patch-management policy and regular server updates *(depending on criticality, the response/fix time is between a few hours and one week)*, and restriction of access for technical staff to resources on a per-need basis.

ADDITIONAL SECURITY CONTROLS

As in any IT framework, security of the system must also be ensured by implementing administrative, technical, and other controls. These controls cover all areas of information security, namely access control, security awareness and training, auditing and accountability, security authorizations, configuration management, contingency planning, authentication, incident response, dealing with equipment maintenance, secure media handling, physical and environmental security, risk management and security planning, personnel security, systems and network security, dealing with supply chain security, and system and information integrity. Seven Bridges maintains an extensive set of documented policies and procedures documenting these controls, available upon request.

II. A HIPAA COMPLIANT PLATFORM FOR ALL CLIENTS

The Seven Bridges Platform is designed to support our clients strict compliance with HIPAA.

The privacy rights of patients in the United States are protected by regulations issued by the Department of Health and Human Services ("HHS") implementing the Health Insurance Portability and Accountability Act ("HIPAA"), including the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule. The HIPAA regulations can be found at 45 CFR Parts 160, 162 and 164; the combined text is available online at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html.

At Seven Bridges we designed our Platform to meet the requirements set by the HIPAA regulations both in order to ensure compliance with regulatory obligations and more generally to ensure the Platform adheres to the highest standards of privacy and security protection.

HIPAA BASICS PART I: WHO'S COVERED AND WHAT'S PROTECTED

The bulk of the HIPAA regulations apply to Covered Entities, which include health insurance plans, healthcare clearinghouses, and healthcare providers which electronically transmit patient information meeting certain standards. A subset of the regulations also apply to Business Associates, which are entities that provide services to Covered Entities or other Business Associates that involve use or disclosure of patient information protected by the regulations. 45 CFR §160.103. When providing services to entities regulated by HIPAA, whether they be Covered Entities or Business Associates, **Seven Bridges plays the role of a Business Associate**.

The HIPAA regulations are designed to protect "Protected Health Information" in the possession of Covered Entities or their Business Associates. Protected Health Information is information that meets two criteria:

- The information relates to the individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual.
- The information identifies the individual or there is a reasonable basis to believe it can be used to identify the individual.

Protected Health Information also includes individual identifiers such as a name or Social Security number when they can be connected to the health information defined above. The HIPAA Privacy Rule also describes methods by which information can be de-identified, bringing it outside the ambit of the regulations. §164.514(a)-(b).

It's worth noting that even if an individual or organization is collecting and using information of a sort that would qualify as Protected Health Information, HIPAA regulations do not directly apply to that individual or organization unless they meet the criteria for Covered Entities or Business Associates. **In particular, data collected for research purposes, even if personally identifiable, is not directly regulated by HIPAA.** However, HIPAA regulations may still have implications for researchers, for instance if their data includes personally identifiable information and is sourced from Covered Entities or Business Associates, or if they are affiliated with regulated entities.

OUR APPROACH: APPLYING HIPAA STANDARDS TO ALL GENOMIC DATA

At Seven Bridges, we have **designed our Platform to go beyond the requirements of the HIPAA regulations in two important ways**.

First, **we treat all of our clients as if they were entities regulated by HIPAA**, providing the same technical protections for their data and abiding by the same stringent policies and procedures. We do this because many clients outside the HIPAA-regulated space find that HIPAA sets a rigorous standard for the sorts of privacy and security protections they need. HIPAA's scope can also sometimes be ambiguous, and some clients may not be sure whether they or their activities are regulated or not. This means that HIPAA Covered Entities or their Business Associates do not need to pay extra for the protections they need, and our other clients get the gold standard for privacy and security protection. *(Clients who know they are regulated by HIPAA should still inform us of this in order to ensure a proper Business Associate Agreement is put in place.)*

Second, **we also treat all client genomic data as Protected Health Information**, even if there is no information included tying that data to a particular individual. We do this because while HHS may not yet treat genomic data as inherently personally-identifiable, we understand that our field is fast approaching the point at which a genome or a subset of it will be able to be reliably linked to a particular individual by third parties. In order to protect our clients and their data subjects from future developments which may render previously-unidentifiable data identifiable, we have decided to treat all genomic data as identifiable from the get-go, providing all the protections associated with Protected Health Information.

HIPAA BASICS PART II: THE RULES AND HOW THE SEVEN BRIDGES PLATFORM ENABLES COMPLIANCE

As noted above, the HIPAA regulations are divided into three main Rules, covering Security, Privacy, and Breach Notification. **The Seven Bridges Platform makes it easy to perform NGS analysis in compliance with these rules**.

SECURITY RULE AT A GLANCE

REQUIREMENT	CFR CITE	COMPLIANCE ON THE SEVEN BRIDGES PLATFORM
Administrative Safeguards	45 CFR §164.308	Seven Bridges has extensive policies and procedures covering all required administrative safeguards, from risk assessment to staff training. Clearance, authorization, and training of client staff is the responsibility of the client, but Seven Bridges can recommend resources if needed.
Physical Safeguards	45 CFR §164.310	Data center security is handled by the cloud infrastructure provider, e.g. AWS, in a compliant fashion. Seven Bridges policies and procedures implement required safeguards for our offices and workstations.
Technical Safeguards	45 CFR §164.312	All required safeguards are implemented on the Seven Bridges Platform, including access controls, audit logging, integrity checks, user authentication and secure transfer of data.
Organizational Requirements	45 CFR §164.314	A Business Associate Agreement (BAA) is in place between Seven Bridges and the cloud infrastructure provider e.g. AWS; Client-Seven Bridges BAAs are available.
Policies and Procedures and Documentation Requirements	45 CFR §164.316	All required policies and procedures are documented and all required documentation is retained for the required minimum of 6 years

The Security Rule lays out requirements designed to ensure the security of patient data. It is split into three main substantive sections, Administrative Safeguards, Physical Safeguards, and Technical Safeguards, alongside sections on organizational and documentation requirements.

The first section lays out required administrative policies and procedures. The most important of these is the requirement that a risk management system be implemented for identifying risks to data security and selecting and implementing controls to address those risks. §164.308(a)(1).

Seven Bridges has a comprehensive risk management program based on the guidelines laid out in NIST Special Publication 800-30.

Other requirements cover implementation of policies and procedures for authorizing access to Protected Health Information, implementation of incident response procedures and contingency plans, and various workforce policies such as required security awareness training, sanctions for privacy and security violations, and policies governing clearance, supervision, and termination of staff members. §164.308(a)(2)-(8). Seven Bridges has internal policies and procedures governing all of these subjects, and the access control features of **the Seven Bridges Platform make it easy for users to implement their own policies for access authorization and control**.

Finally, the administrative safeguards section includes the requirement that Covered Entities put in place agreements requiring their Business Associates to comply with the relevant portions of the HIPAA regulations *("Business Associate Agreements" or "BAAs")*. Business Associates in turn must secure BAAs with any third parties that provide services to the Business Associate involving use or disclosure of Protected Health Information. §164.308(b)(1); See also §164.314(a). **Seven Bridges has entered into a Business Associate Agreement with Amazon Web Services, our provider of cloud-based compute and storage, and stands ready to itself enter into such agreements with any interested clients covered by HIPAA regulations**.

The second section lays out required physical security safeguards. §164.310. Since the Seven Bridges Platform is built on Amazon Web Services, we mostly **rely on the state-of-the-art, more-than-HIPAA-compliant physical security protections at Amazon's data centers** to secure our clients' data. However Seven Bridges has also implemented policies and procedures governing physical access to our offices and workstations, and has defined policies for dealing with data stored on portable media when such storage is required by clients for the transfer of data.

The final substantive section of the Security Rule lays out required technical safeguards, including **access controls, audit logging, integrity checks, user authentication and secure transfer of data**. §164.312. All of these safeguards are integrated in the Seven Bridges Platform by design. § 164.500-530.

PRIVACY RULE AT A GLANCE

REQUIREMENT	CFR CITE	COMPLIANCE ON THE SEVEN BRIDGES PLATFORM
Rules Regarding Use and Disclosure of PHI	45 CFR §164.502-514	Use and disclosure of PHI by Seven Bridges staff complies with rules for Business Associates. Fine-grained access controls make it easy for clients to control use and disclosure by their own staff.
Notices of Privacy Practices	45 CFR §164.520	This is the responsibility of the Covered Entity.
Right to Request Restrictions on PHI	45 CFR §164.522	This is the responsibility of the Covered Entity. However, access controls available on the Platform make it easy to implement requested restrictions.
Right to Access and Amend PHI	45 CFR §164.524-26	Not Applicable - Seven Bridges Platform does not store Designated Record Sets.
Right to Accounting of Disclosures	45 CFR §164.528	Facilitated by the logging features of the Seven Bridges Platform.

The Privacy Rule lays out in detail the ways in which Protected Health Information may be used or disclosed. Business Associates such as Seven Bridges may only use or disclose protected health information as permitted or required by its Business Associate Agreement or as required by law. The Privacy Rule also governs notices of privacy practices and the rights of patients to access their Protected Health Information, request that it be amended, and request an accounting of disclosures. §164.500-530.

Because Seven Bridges does not have any relationship with *(or, typically, any information about)* patients, and all access to, use of, and disclosure of client genomic data on the Seven Bridges Platform is at the direction of the user, compliance with the Privacy Rule is largely the responsibility of the client. However **Seven Bridges has internal policies and procedures in place to ensure client genomic data is only accessed by authorized staff members at the direction of clients or for the purpose of supporting client projects**.

The detailed logs kept automatically by the Seven Bridges Platform can also aid clients in responding to requests for an accounting of disclosures. All logs and other required documentation are maintained for the required minimum of six *(6)* years. See §164.316.

BREACH NOTIFICATION RULE AT A GLANCE

REQUIREMENT	CFR CITE	COMPLIANCE ON THE SEVEN BRIDGES PLATFORM
Notification by Business Associate	45 CFR §164.410	Seven Bridges has policies and procedures providing for investigation of breaches and required notification of clients
Notification to Individuals, the Media and HHS	45 CFR §164.404-408	This is the responsibility of the Covered Entity.

The final Rule is the most narrow, dealing specifically with notifying patients of security breaches involving their Protected Health Information. §164.400-414. **Seven Bridges has a comprehensive policy for investigation of potential security breaches and notification of affected clients**. The policy requires all investigations to be documented in writing and all documentation to be retained for a minimum of six (6) years. All members of the Seven Bridges staff are trained on the policy.

Because Seven Bridges will not have a relationship with individual data subjects and frequently will not even have information regarding their identities, in most instances further notifications including ultimate notification of patients will be up to the client. See §164.410.

If you're interested in learning more about HIPAA compliance on the Seven Bridges Platform, we encourage you to contact any member of our sales team or write to our Privacy and Security team directly at security@sbgenomics.com. We would be happy to provide our documented policies and procedures as well as a detailed breakdown of how we meet individual HIPAA requirements to clients or potential clients upon request.

III. ISO/IEC 27001:2013 CERTIFICATION

ISO/IEC 27001:2013 is part of the ISO/IEC 27000 family of international information security standards, backed up by third-party audits and certification by an accredited certification body. The standard mandates a rigorous, risk-based approach to information security while offering organizations flexibility to tailor their controls to their operating environment and risk profile. While ISO certification is not required by law or regulation, it provide clients assurance that our information security management system has been evaluated by a trusted third party and found to meet the highest industry-agnostic certifiable information security standard in the world.

An ISO 27001 certificate (and the audit process it is based on) is limited to a defined scope, setting out what information systems are covered. As you'll see on our ISO certificate, we defined our scope broadly to ensure our clients' information is protected:

The scope of the ISO/IEC 27001:2013 certification is limited to the information security management system (ISMS) supporting cloud-based environments and related information systems owned or operated by Seven Bridges for the management of its own information

assets and those of its clients and business partners, in accordance with the statement of applicability version 1.2, dated July 14, 2017.

On this basis, our information security team conducts regular risk assessments and maintains a risk register identifying a wide range of risks to in-scope information systems and mapping out technical and organizational controls mitigating those risks. The controls are largely selected from Annex A to the ISO 27001 standard, which lists out 114 controls broken out into 35 control categories, covering everything from cryptography and secure development to employment practices and vendor management. The overall risk profile is subject to review by executive management and the entire system is subject to regular internal audits as well as annual external surveillance audits by a third-party accredited certification body.

Our ISO 27001 certificate is publicly available on the website of our third-party accredited certification body at https://cert.schellmanco.com/?certhash=SSBx0FZtsrvd.

IV. COMPLIANCE WITH DATA PROTECTION LAWS, INCLUDING THE GDPR

THE EU DATA PROTECTION REGIME

While the United States prefers to protect privacy rights through industry-specific rules such as HIPAA, jurisdictions such as the European Union have taken a more comprehensive approach to the protection of personal data. Seven Bridges stands ready to ensure our clients can use our platform in full compliance with local data protection laws. Below we outline our compliance with European data protection laws, as the EU has developed a data protection regime that provides an optimal framework for key privacy and security considerations .

The foundation of the European data protection regime is the General Data Protection Regulation (GDPR), which lays out a detailed set of obligations intended to unify the data protection laws of European countries and reinforce commitments to European data subject privacy by strengthening the rights of citizens with regards to their personal data.

KEY ROLES UNDER THE GDPR

There are four key actors that one should consider when thinking about GDPR compliance: **data subjects, data controllers, data processors**, and **supervisory authorities**. Data subjects are those persons from which personal data is collected. Personal data is defined in Article 4(1) of the regulation as "any information relating to an identified or identifiable natural person." This broad definition means that personal data can be anything from genetic information to a government-issued unique identifier.

Most obligations outlined in the GDPR are directed at data controllers and data processors. The data controller determines the purpose of the processing of the personal data, with "processing" being broadly defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means." Data processors, on the other hand, process the personal data at

the direction of the data controller and do not make any decisions whatsoever about the purpose of processing.

KEY ACTOR	ROLE	SCOPE
Data Subjects	Their data is processed	Data Subjects are living, natural persons
Data Controllers	Determines the purpose of processing of EU personal data	The GDPR is applicable: - Where the Data Controller is established in the EU or a country where Member State law applies - Where, regardless of where the Data Controller is established, the processing of EU data subject data relates to the offering of goods or services or the monitoring of behavior
Data Processors	Processes EU personal data on behalf of the Data Controller	The GDPR is applicable: - Where the Data Processor is established in the EU - Where the processing of EU data subject data relates to the offering of goods or services or the monitoring of behavior
Supervisory Authorities (Data Protection Authorities)	Promote, monitor, and enforce the GDPR through awareness activities, investigations, annual reports, and the protection of human rights	Each EU Member State has an active Data Protection Authority

The supervisory authorities defined in the GDPR are represented in the form of each member state's Data Protection Authority (DPA). DPAs have a broad set of responsibilities that allow them to monitor and correct the activities of data controllers and data processors. They are also the primary points of contact when a Data Subject wants to escalate a grievance against a data controller or data processor.

Seven Bridges operates as both a Data Processor and a Data Controller.

As Data Processor:

- We process genomic data at the direction of our clients - the Data Controllers

for the genomic data.

As Data Controller, we collect the following types of information:

- Platform registration information (e.g. login, email address, phone number)
- Platform user activity

- Datasets we make available to our users

COMPLIANCE AS DATA PROCESSOR

Seven Bridges works with all of its clients to determine if the service provider agreements it enters into with its clients necessitate key contractual provisions mandated by the GDPR. Specifically, where Seven Bridges (data processor) or the client (data controller) believe Seven Bridges is processing EU citizen data on behalf of the client, the following provisions are included in our service provider agreements:

- Description of processing
- Documented instructions for the data processor
- Confidentiality guarantees from the data processors
- Guarantee from the data processor to implement appropriate technical and organizational measures for security
- An authorization to use subprocessors/subcontractors where necessary
- A guarantee to flowdown any obligations of data processor to subprocessors
- A subcontracting liability clause
- A commitment to assist the data controller with any requests from Data Subjects
- A commitment to assist the data controller with responding to data breaches
- A commitment to assist the data controller with Data Protection Impact Assessments as necessary
- Outlines of policies for data deletion and data returns
- Data controller audit rights
- A commitment to only initiate international transfers outside of the European Economic Area at the request of the data controller

The technical security measures we mention in this white paper (and our Security White Paper), written data access protocols, and standard operating procedures for responding to compromised systems all allow us to comply with the contractual provisions listed above. All of our subprocessors undergo thorough reviews by our legal, privacy, and security teams to ensure they employ practices and systems that meet the same standards that Seven Bridges uses to fulfill our obligations to clients for which we are a data processor.

COMPLIANCE AS DATA CONTROLLER

For Platform user data, Seven Bridges uses the Privacy Policy available on our website to inform users about a) the types of personal data we may collect from them, b) what we do with that data (type of processing), and c) the legal basis for processing of the data. Because Seven Bridges determines the purpose of platform user data, we are the data controller for such data. Similarly, we issue privacy notices to our employees in the European Economic Area to let them know the types of data we may need to collect from them and process in order to carry out the terms of their employment contracts.

As data controllers, we employ the same security and organizational measures that we employee in the services of our clients; however, we also take some additional steps to ensure we are complying with any additional obligations the GDPR places on data controllers. For example, we conduct internal Data Protection Impact Assessments of our own on any data in our data inventory for which we believe we are the data controller. We also are refining our procedures for communicating directly with Data Protection Authorities or other supervisory entities should we need to respond to an inquiry as data controller.

INTERNATIONAL TRANSFERS

Transfers of European citizen data outside of the European Economic Area (EEA) require a legal mechanism accepted and approved by the European Commission. Under the General Data Protection Regulation's predecessor, the European Directive 95/46/EC, the European Commission was granted the right to approve what have become known as the EU Model Clauses as one such mechanism. Seven Bridges includes the EU Model Clauses in contracts governing its processing of data that it transfers outside of the EEA. We have also self-validated as a requirement of the EU-U.S. Privacy Shield since 2016 for data transfers from the EEA to the United States.

THE EU MODEL CLAUSES

Article 26 of the Data Protection Directive empowers the European Commission to approve model contract clauses which are deemed to provide adequate protection for transferred data by imposing requirements on all parties ensuring compliance with the key requirements of the Directive. The EU's Information Commissioner has promulgated two sets of model clauses pursuant to this authority, one covering transfers between data controllers and one covering transfers from a data controller to a data processor which will process that data on behalf of the controller.

The clauses include requirements identical to those Seven Bridges puts into its service provider agreements with those clients for which it is processing EU citizen data. Importantly, the clauses also allow individual data subjects to enforce those clauses which are intended to protect their data, a right of enforcement that extends to the data exporter, the data importer, and any subprocessor. The data importer is also required to inform the exporter of any disclosure of data which may be compelled by law as well as any laws applicable to it which may have a substantial adverse effect on its ability to carry out its obligations under the model clauses.

Seven Bridges stands ready to include the model contract clauses in any agreement with EU-based clients in order to help them meet their data protection obligations. We have already agreed to data processing addendums with our subprocessors--including our cloud infrastructure providers--which include the model clauses and allow us to ensure subprocessor compliance where international transfers are necessary.

THE EU-U.S. PRIVACY SHIELD

While U.S. law in and of itself is not deemed to provide "adequate" protection in the case of international transfers, there are other mechanisms by which adequate protection for

transferred data may nonetheless be achieved. The most robust and commonly accepted of these is the EU-U.S. Privacy Shield framework, of which Seven Bridges is a member. Privacy Shield replaced the Safe Harbor framework, which the European Court of Justice invalidated in 2015 over concerns of U.S. government access to corporate data.

As participants in Privacy Shield, we are required to clearly describe how we collect and process data in our Privacy Policy as well as adhere to the Privacy Shield Principles, which echo the requirements of the General Data Protection Regulation.Any EU data subject can file a complaint directly with our, which must respond within 45 days. They may also pursue the matter through their national Data Protection Authority, or through Seven Bridges' identified independent recourse mechanism, the Better Business Bureau. Binding arbitration may also be available. Companies who fail to honor their obligations under Privacy Shield may incur a range of penalties under law.

Seven Bridges' participation in Privacy Shield is overseen by the International Trade Administration of the United States Department of Commerce. To verify our Privacy Shield participation and learn more about our privacy practices, please see our public Privacy Shield registration page.

THE PRIVACY SHIELD PRINCIPLES AND SEVEN BRIDGES

At Seven Bridges, we believe the Privacy Shield Principles represent a common sense approach to the stewardship of personal data and we take our commitment to abide by them quite seriously. We comply with each of the Principles in the following ways:

- **Notice**: The Notice principle requires notice of what personal data we collect and how we use it. We provide notice to our users via a Privacy Policy, available at https://www.sbgenomics.com/privacy-policy/.
- **Choice**: The Choice principle requires us to allow data subjects to opt out of use or transfer of their data that is inconsistent with the purpose for which it was collected. We comply with this Principle by providing users with fine-grained controls on how their data is shared with other users and by only using user information to provide and improve our service.
- **Onward Transfer**: The Onward Transfer principle requires us to abide by the Notice and Choice principles when transferring data to third parties, and to ensure that these parties themselves have adequate privacy protections. We comply with this principle by only providing data to third parties for the purpose of providing and improving our service, by noting in our Privacy Policy when data may be provided to third parties, and by vetting third parties' privacy and security protections before entrusting them with data.
- **Security**: The Security principle requires us to implement procedures and technical protections to ensure data is kept secure. We comply with this principle through the measures described in this white paper and the Seven Bridges Security White Paper.
- **Data Integrity**: The Data Integrity principle requires us to ensure that the data we keep is relevant, accurate, current, and generally adequate for the purposes for which it was collected. We comply with this principle by keeping the data we collect on users to the minimum necessary to provide and improve our service.
- **Access**: The Access principle requires us to provide data subjects with reasonable

access to the data we have collected. In our Privacy Policy, we describe how users can access the data they have submitted to us. Access requests for other data we may have collected (for instance, via the sales process) or requests for access by non-user data subjects may be directed to dpo@sbgenomics.com.

- **Enforcement**: While the Privacy Shield Framework encourages data subjects to resolve disputes directly with participating companies, it recognizes that sometimes a third party needs to step in. This principle requires us to arrange for such a third party to provide an independent dispute resolution mechanism for privacy complaints. To meet this requirement, we have turned to the Better Business Bureau's Privacy Shield Dispute Resolution Program, which you can learn more about at http://www.bbb.org/EU-privacy-shield/.

OUR DATA PROTECTION OFFICE

Further questions about our privacy and data protection practices should be directed to our Data Protection Officer at dpo@sbgenomics.com. Our team, which holds CIPM and CIPP/E certifications from the International Association of Privacy Professionals is trained to assist you with a range of topics.

V. ENABLING COMPLIANCE WITH dbGaP SECURITY BEST PRACTICES

WHAT dbGaP SECURITY BEST PRACTICES ARE AND WHO THEY APPLY TO

The dbGaP Security Best Practices are a set of requirements that must be met by researchers who use the "controlled-access" tier of datasets included in the database of Genotypes and Phenotypes (dbGaP).

Researchers wishing to analyze controlled-access human genomic and phenotypic data in NIH-designated repositories governed by the NIH Genomic Data Sharing Policy (such as TCGA) are required to enter into Data Use Certification (DUC) Agreements with the NIH setting out the conditions under which they are allowed to access, store, and use the data in these databases. These conditions include adhering to a security plan that meets the requirements of the Security Best Practices, which set out general requirements for securely working with sensitive genetic data. The latest update to the Security Best Practices, published in March 2015, also specifically addresses security concerns particular to working in the cloud.

The dbGaP Security Best Practices are available at https://osp.od.nih.gov/wp-content/uploads/NIH_Best_Practices_for_Controlled-Access_Data_Subject_to_the_NIH_GDS_Policy.pdf.

Before using the Seven Bridges Platform to store or analyze controlled-access data, researchers should update their Data Access Request to specifically indicate the use of the Seven Bridges Platform as a cloud computing service. While the institution retains ultimate responsibility for information security in cloud environments, features of the Seven Bridges Platform can facilitate compliance with security requirements. The following information

is meant to provide guidance for how **the Seven Bridges Platform can facilitate secure and compliant use of controlled-access data in the cloud.**

dbGaP SECURITY COMPLIANCE AT A GLANCE

General Information Security Guidelines	The Seven Bridges Platform provides data isolation, complete access control, and user authentication.
Physical Security Guidelines	Storing data on the cloud with the Seven Bridges Platform obviates the need for portable media or building facilities with restricted physical access.
Controls for Servers	The Seven Bridges Platform is deployed within Virtual Private Clouds and access to physical data centers is controlled by our infrastructure providers' state-of-the-art security measures. The platform allows tight control of data access throughout the data analysis life cycle and the principle of Least Privilege is enforced by default.
Source Data and Control of Copies of Data	The Seven Bridges Platform provides a robust provenance and logging system to manage not only the original files, but also any files resulting from computational analysis.
Destruction of Data	A strict data purging policy ensures that all data used transiently during computation (for example on EC2 instances) is immediately deleted following its use. Data stored on S3, including original files and those resulting from computational analysis can be easily and fully destroyed by authorized users when these files are no longer needed.
General Cloud Computing Guidelines	All data in the Seven Bridges Platform is encrypted both during transfer and at rest. Inbound access is restricted using Virtual Private Clouds which are configured with the minimum ports necessary for each application. Regular vulnerability scanning and penetration tests ensure that the system is always protected against even emergent threats.
Audit and Accountability	The Seven Bridges Platform provides fine-grained access control and allows investigators to set and continually monitor user permissions.
Image Specific Security	Seven Bridges manages server provisioning and management by using infrastructure-as-a-code approach and modern configuration management tools, so any server can be rebuilt in a couple of minutes according to a certain policy. This policy handles secure base configuration of servers, regular patches and controlled change management.

IMPLEMENTING dbGaP SECURITY BEST PRACTICES USING THE SEVEN BRIDGES PLATFORM

The Seven Bridges Platform allows for easy compliance with all relevant dbGaP standards.

The Best Practices document provides guidance for individuals in the following roles: scientific staff making use of the data, and IT staff setting up the necessary computing infrastructure. Each section also contains a subsection on using cloud computing resources like the Seven Bridges Platform. The Seven Bridges Platform meets or exceeds all the

standards for working with controlled data in cloud-based environments.

BEST PRACTICES FOR SCIENTIFIC STAFF

The section of Best Practices directed at scientific staff emphasizes the importance of establishing a formal security plan to control access to and use of data. While the Best Practices rightly emphasize that setting up a security plan is the responsibility of researchers and their institutions, the Seven Bridges Platform has a number of features which actively guide users toward creating a compliant security plan.

The Best Practices emphasize that security should be "on by default", and be built on a strong foundation of access controls and accountability. On the Seven Bridges Platform, both are the case.

A user's data is private by default, and fine-grained access controls allow users to grant their collaborators the minimum permissions necessary for their roles. Individual users are required to set up their own strong passwords and all activities are logged, allowing for accountability. Storing your data on the Seven Bridges Platform also makes it easy to avoid the use of portable media, which the Best Practices discourage, and delete all the data as required at the end of your project.

BEST PRACTICES FOR IT STAFF

The section of the Best Practices directed at IT staff contains more detailed recommendations for technical security controls. The Seven Bridges Platform supports all of the recommended controls.

While most are Platform defaults -- IT staff get them "automatically" -- the rest are easily enabled on an as-needed basis.

The first set of recommendations for IT staff consist of general guidelines. The Best Practices require that data not be posted publicly or available on the web, that external access to cloud instances and storage be restricted, and that software patches be up to date, all of which is handled automatically by the Seven Bridges Platform. Seven Bridges also makes it easy to set strong passwords.

The next set of recommendations deal with physical security and controls for servers, and again, Seven Bridges meets them all. On the Platform, your data is stored and processed in cloud provider data centers with state-of-the-art physical security protections. The required server controls are implemented by Seven Bridges, including enforcement of the principle of Least Privilege on the process level, use of VPN for remote access to the production environment, and retention of data access controls throughout processing. Fine-grained access controls on the Seven Bridges Platform allow researchers to implement the principle of Least Privilege on the individual user level, restrict downloading of data and provide "view only" access as needed.

The final sets of recommendations deal with logging and destruction of data. The Seven Bridges Platform automatically logs all user activity, making it easy to keep track of copies of data and what is done with it. All logs are stored for a minimum of six (6) years. It also makes it easy to delete data, with all data automatically purged from all systems and backup copies destroyed within a week.

CLOUD COMPUTING

As the advantage of of cloud computing for bioinformatics is now clear, the March 2015 version of the Best Practices for the first time included requirements and recommendations specific to users of cloud computing environments.

As with the general requirements, on the Seven Bridges Platform everything needed for complete compliance is already implemented for you, or ready to be enabled. All data transfer to and from the Platform is conducted over HTTPS exclusively. Inbound access to computational instances is restricted using Virtual Private Clouds, the security profile of these instances is configured to allow access only to the minimum set of ports required to provide necessary functionality for your services, administrative access is restricted to the minimum set of ports and source IP address ranges necessary, and the image specific security requirements are all met.

The user-and-project-specific access control features and extensive logging performed by the Seven Bridges Platform also make it easy to review Access Control Lists and logs of individual user activity. While the Seven Bridges Platform allows researchers to readily comply with dbGaP security policies, users retain ultimate control and responsibility for access to their projects and data.

VI. CLIA AND CAP COMPLIANCE

Laboratory testing performed on specimens from humans for the purpose of diagnosis, prevention, or treatment of disease or assessment of health is governed by regulations issued by the Centers for Medicare & Medicaid Services under the authority of the Clinical Laboratory Improvement Amendments of 1988, as amended ("CLIA Regulations").

The CLIA regulations establish quality standards for all laboratory testing to ensure the accuracy, reliability and timeliness of patient test results regardless of where the test was performed. They include quality standards for proficiency testing (PT), patient test management, quality control, personnel qualifications and quality assurance.

But while CLIA regulations set the baseline standard for clinical labs, many clinical labs instead choose to have their practices evaluated under more rigorous standards set by the College of American Pathologists ("CAP"), considered the gold standard for clinical laboratory practices. From a regulatory perspective, because CAP standards have been recognized as going above and beyond what is required by CLIA regulations, accreditation by CAP is formally "deemed" by CMS to certify compliance with CLIA regulations as well.

At Seven Bridges we have experience working with clients to ensure compliance with CAP and CLIA standards and are happy to assist labs in setting up compliant policies and procedures.

VII. FDA

Some of our clients may find that their use of the Platform is subject to U.S. Food and Drug Administration (FDA) regulations. In some cases this may be because data produced using the Platform will ultimately be submitted to the FDA, e.g. to support a new drug application, and so is subject to the FDA's regulation regarding electronic records, 21 CFR Part 11. In other cases, the Platform may be used as part of processes subject to FDA quality systems regulations, bringing it within the scope of the FDA's guidance on software quality and validation. For clients in these situations, the Platform is designed to allow clients to meet their compliance obligations.

21 CFR PART 11

The Platform has all the features necessary for clients to comply with the record-keeping requirements of 21 CFR Part 11:

- **Development and Validation:** The Platform is developed by trained software engineers under the guidance of expert bioinformaticians (§11.10(i)) in accordance with documented quality assurance procedures to ensure validation of system functionality (§11.10(a)).
- **Pipeline Specification and Reproducibility**: The Platform uses the Common Workflow Language to fully document all components and parameters of data analysis pipelines, allowing for verifiable validation of client pipelines, automatic enforcement of operational checks to ensure proper pipeline execution, and reproducibility of all data generated (§11.10(a), §11.10(b), and §11.10(f)).
- **Data Storage**: All client data is stored and transmitted in encrypted form, backed up regularly, and retained by default for a minimum of 6 years. Checksums are used to ensure integrity of data (§11.10(b), §11.10(c), and §11.30).
- **Access Control**: The Platform's permissions system allows clients to limit access to the Platform to authorized and trained personnel, as well as exercise more fine-grained control over user permissions (such as allowing some users to access data but not alter it), further protecting data integrity (§11.10(d) and §11.10(i)).
- **Authentication**: User authentication can be accomplished using the Platform's built-in authentication features or through integration with a client's SSO solution using SAML2 (§11.10(g)).
- **Auditability**: Seven Bridges maintains audit trails that are available upon request (§11.10(e)). Finally, Platform documentation is available to all users online and version-controlled by Seven Bridges (§11.10(k)).

While the Platform currently does not support electronic signatures (§11.50-§11.300), in most cases records maintained on the Platform need not be signed under the predicate rules, and in any case signature requirements can be met through integration with other information systems or via a "hybrid" approach.

QUALITY SYSTEM REGULATION AND SOFTWARE VALIDATION

Certain provisions of the Quality System regulation apply to the validation of:

- Software used as a component of a medical device;
- Software that is itself a medical device;
- Software used in the production of a device; and
- Software used in implementation of the device manufacturer's quality system.

The FDA defines software validation as "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled." Seven Bridges has established software validation practices in line with recommendations referenced in the FDA's General Principles of Software Validation; Final Guidance for Industry and FDA Staff, Version 2.0 (http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm).

The FDA sees a documented user requirements specification defining a software's "intended use" as one of the key elements of software validation. Seven Bridges' Software Development Lifecycle (SDLC) documentation requires that all product and feature design documents include functional specifications describing how the proposed solution will meet user requirements (e.g. performance requirements, safety requirements, requirements dictated by the intended operating environments). Design specifications documents also include risk assessments.

TEAM@SEVENBRIDGES.COM
SEVENBRIDGES.COM

SevenBridges