Security, Privacy, and Regulatory Compliance White Paper

The purpose of this white paper is to inform users about SkyGenic's security and privacy framework. Storing and computing genomic data on SkyGenic's Platform enables its users to be compliant with the different global regulatory requirements that encompass their research and scientific progress.

Table of Contents

Introduction

At SkyGenic, we are proud to be part of the exciting advances in the field of genomics that has occurred in recent years. SkyGenic has undertaken the responsibility of providing their users with a secure environment that they can control for the storage and computation of their genomic data. This allows users to concentrate on their research and changing lives rather than worrying about system setup, security, or regulatory requirements. Our developers, security experts, and advisors have invested years in the creation of SkyGenic and its architecture to ensure that it not only fulfills the user's immediate needs but also anticipates future requirements.

SkyGenic's architecture can be apportioned into two broad categories: the software that was developed to create the SkyGenic Platform and the hardware/software combination that make up the infrastructure on which SkyGenic resides. These two areas combine to provide end-to-end security and data privacy over which users have complete control.

SkyGenic Security Infrastructure and Framework

As a cloud-based platform for genomic storage and computation, SkyGenic takes advantage of the existing infrastructure, software, resources, and compliance that Google Cloud Platform has to offer. As a global cloud infrastructure provider, Google's team of more than 700 security personnel are able to provide a secure environment matched by few other companies worldwide. Their envelope encompasses physical security of their data centers, hardware design for redundancy, encryption of data at rest and transit, privacy safeguards, and a variety of other services too vast to mention. For more in-depth knowledge of Google's infrastructure, security, deletion policies, and approach to genomic data, the following links are provided:

Google Cloud Platform

Google infrastructure security design overview

Google security whitepaper

Data deletion on Google Cloud Platform

Handling genomic data in the cloud

SkyGenic Platform Architecture

Building SkyGenic on the Google Cloud Platform alone does not ensure a safe and secure platform. Appropriate design, architecture, and safeguards are required for a complete environment.

Data security at rest and transit

For data to be considered secure, it must be isolated and contained with access only provided to authorized users. The two states that data can be found are either at rest or in transit between locations. At rest can be short term, long term, or within a virtual machine for computational purposes. In transit is either from the user's storage location or a third party cloud location into SkyGenic or from an at rest location to another at rest location within the SkyGenic Platform. Once within the Google Cloud Platform envelope, data at rest and in transit are encrypted as indicated in Google's white papers (Encryption at rest in Google Cloud Platform, Encryption in transit in Google Cloud). Data transfers into SkyGenic are exclusively through SSL/TLS dedicated channels; Figure 1 depicts data flows within SkyGenic.

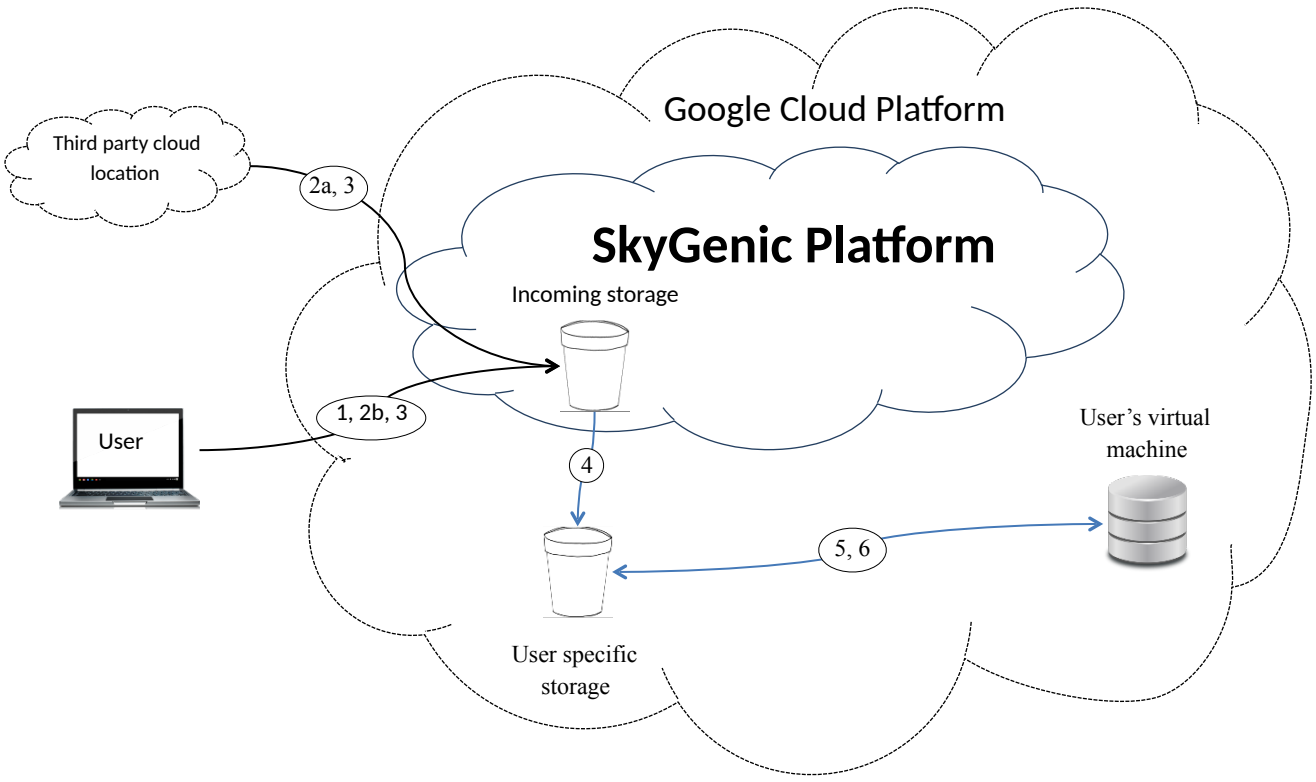

Figure 1. Data flows within SkyGenic

1) User signs into the SkyGenic Platform and a unique identifier is assigned for the session
2) A secure TLS connection is established with the SkyGenic Platform
    a) TLS connection is between another cloud location and SkyGenic incoming storage
    b) TLS connection is between a user's on premises computer and SkyGenic incoming storage
3) A file is transferred into SkyGenic's incoming storage, the user's identifier is verified, and a checksum guarantees file completion
4) The verified file is transferred into a user's specific storage container
5) When the user requests a computation, SkyGenic starts a virtual machine specific to the user and transfers the files into it
6) When the computation is complete, the files and outputs are transferred to the user's storage container. After a checksum verifies data integrity, the virtual machine and all information is deleted.

Authorization and access

Although files are fully encrypted within the SkyGenic Platform, appropriate authorization and access needs to be established. Users log into the SkyGenic Platform with their chosen email address and secure password. It is the user's responsibility not to share or allow their login information to be obtained by others.

A file, owned by the user, is uploaded into SkyGenic. The owner has the ability to share the files with other users, modify access permissions at any time, or revoke access that was previously provided. Ownership of a file can also be transferred to another user within SkyGenic at any time. It is the owner's responsibility to share protected health information only with other users that have legally authorized access to view or use the files.

Audit logging

SkyGenic maintains audit logs for 6 years to ensure HIPAA regulatory compliance. These audit logs document all file activity within SkyGenic and are stored outside the SkyGenic Platform to ensure their integrity should a breach of SkyGenic occur. Once a daily log is created, it cannot be modified for the 6-year retention period.

Malicious activity

SkyGenic's architecture was specifically designed to prevent malicious activity. The points of entry, where someone would attempt to breach the platform, have multiple checks and

safeguards. The OWASP Top 10 web application security risk prevention techniques have been adopted and incorporated into the security architecture.

1. Injection
2. Broken authentication and session management
3. Cross-site scripting (XSS)
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function level access control
8. Cross-site request forgery
9. Using components with known vulnerabilities
10. Unvalidated redirects and forwards

The audit logs along with other tools are used for regular evaluation of the platform to look for suspicious activity or security breaches. This architecture along with Google Cloud's security features are combined to minimize the risk of a breach ever occurring.

HIPAA Compliance

To protect the rights of patients within the United States, the Department of Health and Human Services (HHS) enacted the Health Insurance Portability and Accountability Act (HIPAA) that regulates storage and use of a patient's information and medical records. CFR title 45 parts 160, 162 and 164 comprise the HIPAA act that is available on the HHS website (HIPAA combined regulations)

The SkyGenic Platform is designed to be fully HIPAA compliant to ensure that users can store any protected health information (PHI) that is needed. As defined in 45 CFR 160.103, SkyGenic performs the role of a business associate for its users and clients. SkyGenic is designed to provide its users with granular control of their information and files. If SkyGenic is used to share files, it is the owner's responsibility to ensure that only authorized personnel are provided access.

For researchers, it can at times be ambiguous whether their patients' genomic data or associated information falls under HIPAA regulations. HIPAA regulations describe how patient information can be de-identified (45 CFR 164.514), allowing it to fall outside of HIPAA requirements. Whether a patient's complete or partial genomic data is considered protected health information is still being discussed. For this reason and to anticipate PHI requirements that may develop in the future, SkyGenic is designed so that all stored data fulfills HIPAA requirements.

SkyGenic will enter a custom business associate agreement with users upon request; inquiries can be sent to info@SkyGenic.com. By creating a SkyGenic user account by default, the user agrees to SkyGenic's business associate agreement.

The HIPAA regulation is composed of three distinct sections; the security rule, breach notification rule, and privacy rule. The security rule outlines administrative, physical, and technical requirements that need to be implemented to keep the data stored in a safe and secure environment. The breach notification rule has specific procedures and requirements that need to be followed should a breach of information occur. Since SkyGenic is a business associate and does not have direct contact with patients, most of these requirements fall under the responsibility of the user. The final section is the privacy rule which governs how PHI may be used or disclosed to others. SkyGenic can only use or disclose PHI as specifically outlined in the business associate agreement and in the HIPAA regulation. Because users have granular control of their data within SkyGenic, it is primarily their responsibility to comply with the security rule and only disclose PHI to other users with appropriate access. The following table provides a brief outline of the most relevant sections and SkyGenic's approach to fulfilling the requirements.

Security and Privacy

Standard	Section	SkyGenic Implementation
Administrative Safeguards	164.308	SkyGenic and Google have internal policies and procedures to fulfill the requirements of HIPAA's administrative safeguards. This includes but is not limited to system risk assessment and security, employee access management, and response procedures.

Physical Safeguards	164.310	Facility access, device, and media controls are the responsibility of Google, the cloud platform on which SkyGenic resides. Google has multiple white papers indicating how these requirements are fulfilled. SkyGenic has internal policies and procedures safeguarding access to PHI data through its workstations.
Technical Safeguards	164.312	SkyGenic's Platform implements all required technical safeguards including user authentication, automatic logoff from inactivity, activity logging, emergency data access, encryption, and data integrity verification.
Organizational Requirements	164.314	SkyGenic has entered into a Business Associate Agreement (BAA) with Google and by default enters into SkyGenic's BAA agreement with the user. Upon request, SkyGenic will enter into a custom BAA agreement with a user or the organization to which they belong.
Policies and Procedures and Documentation Requirements	164.316	SkyGenic has internal documents and procedures implemented within its organization to fulfill all requirements. These documents are updated as necessary and maintained for a minimum of 6 years.

Breach Notification

Standard	Section	SkyGenic Implementation
Notification to Individuals, the Media, and the Secretary	164.404-164.408	Notification of the required parties is the responsibility of the user. SkyGenic, as a business associate, does not have access to patient information.
Notification by a Business Associate	164.410	SkyGenic is treated as a business associate to the user, and as such, does not have access to individual patient information. Should a breach occur, SkyGenic will contact users affected within the allotted 60 days and provide access logs and breach information as required.

Privacy of Individually Identifiable Health Information

Standard	Section	SkyGenic Implementation
Uses and Disclosure of PHI	164.502-164.514	SkyGenic complies with all rules and requirements of PHI for Business Associates. Users have fine-grained control and are responsible for use and distribution of PHI only to authorized individuals or organizations.
Notification by a Business Associate	164.520	SkyGenic is treated as a business associate to the user and as such does not have access to individual patient information. Should a breach occur, SkyGenic will contact users affected within the allotted 60 days and provide access logs and breach information as required.
Notification to Individuals, the Media, and the Secretary	164.522	Notification of the required parties is the responsibility of the user. SkyGenic as a business associate does not have access to patient information.

Notification by a Business Associate	164.524-164.526	SkyGenic is treated as a business associate to the user and as such does not have access to individual patient information. Should a breach occur, SkyGenic will contact the users affected within the allotted 60 days and provide access logs and breach information as required.
Accounting of Disclosures of PHI	164.528	SkyGenic's access logs fulfill these requirements and are available for the required period of 6 years.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the regulatory law for the data protection and privacy of the European Union, United Kingdom and the European Economic Area's residents. In contrast to HIPAA requirements that are specific to healthcare, the GDPR is a broad regulatory requirement designed to facilitate uniformity across the European Union and provide its citizens with control over their personal data, not necessarily medical in nature. SkyGenic was designed to allow its users to be in full compliance with the European data protection laws.

There are four areas that govern the GDPR: the data subjects, data controllers, data processors and supervisory authorities. The data subjects are the European Union citizens whose identifiable information was collected for processing and analysis. This includes genomic data even if no other patient information is retained because it is uniquely identifiable. The data controllers of the patient's data are SkyGenic users who have direct control over processing and analysis. Within SkyGenic, there are no automated analysis processes that occur; analysis control is entirely by the user. For users located in the European Union, SkyGenic collects their registration and user information such as name, email address, and phone number thus acting as the data controller for them. SkyGenic and the Google Cloud Platform fulfill the role of the data processor, providing the environment for the data controllers. Finally, there is the supervisory authority that monitors and enforces the GDPR.

As data controllers, it is the SkyGenic user's responsibility to obtain legal consent from data subjects to use their identifiable genomic data. The SkyGenic Platform provides an environment allowing the user/data controller to restrict the region where the data will be stored and analyzed. This fulfills the requirement that European Union citizens' identifiable information must remain within the country of origin unless model contract clauses are obtained.

GDPR Roles and Responsibilities

GDPR Role	Identified Party	Implementation
Data Subject	Genomic sample of EU citizen SkyGenic User	**EU citizen:** Genomic samples are collected for research purposes by the data controller. **SkyGenic User:** To use the SkyGenic Platform, the user provides registration information such as name, email address, employer, and billing information.
Data Controller	SkyGenic User SkyGenic/Google/Third-Party Vendor	**SkyGenic User:** The SkyGenic user has fine-grained control over a data subject's genomic data including removal of it completely from SkyGenic. **SkyGenic/Google/Third-Party Vendor:** A user's activity and registration information are collected for platform use or to improve a user's experience. A user's account is removed upon request.
Data Processor	SkyGenic/Google	**SkyGenic/Google:** Data is not processed automatically; the user as the data controller has complete control over a data subject's genomic information.
Supervisory Authority	Respective EU state's authority	Each EU state has their own Data Protection Authority designated with regulation and enforcement of GDPR.

The EU-U.S. and Swiss-U.S. Privacy Shield

SkyGenic is a participant of the EU-U.S. and Swiss-U.S. Privacy Shield, a mechanism that verifies adequacy and allows the transfer of EU and Swiss citizens' personal information into the U.S. As participants, we have implemented the Privacy Shield Principles, which require the participant to clearly state what information is collected and how it is used within our Privacy Policy.

Privacy Shield Principles

Principle	SkyGenic Fulfillment and Implementation
Notice	SkyGenic complies with this principle by notifying users regarding what personal data is collected and how it is used within this white paper and SkyGenic's privacy policy.
Choice	SkyGenic's users have fine-grained control of their data. It is their responsibility and control to share files only with other SkyGenic users who have legal permission. User's information that SkyGenic collects directly is only used to improve their experience and our service to our customers.
Accountability for Onward Transfer	SkyGenic only provides user's information or data to third parties for providing and improving our service to the user (for example, billing information to a third-party service for bill payment purposes). All third parties' privacy and security policies are vetted and evaluated prior to using their services.
Security	SkyGenic's framework provides technical safeguards for user's data along with policies and procedures for a secure environment. Additional information can be found in SkyGenic's Security White Paper.
Data Integrity and Purpose Limitation	Data collected on and from users is only obtained and used to improve their experience and our service to our customers. Any irrelevant information or data is not collected.
Access	Upon request, users can obtain information provided or collected by SkyGenic that is associated with their user account. Direct all inquiries to dpo@SkyGenic.com
Recourse, Enforcement and Liability	Any concerns by a user should first be directed to dpo@SkyGenic.com. Should any unresolved issues remain after contacting SkyGenic directly, the Better Business Bureau's Privacy Shield Dispute Resolution Program will be provided free of charge as an independent dispute resolution mechanism. Additional information can be found at www.bbb.org/EU-privacy-shield/for-eu-consumers

SkyGenic's Data Protection Officer

Additional questions about SkyGenic's security, privacy, or regulatory compliance should be directed to our Data Protection Officer at dpo@SkyGenic.com.