Genes and Health Researcher Code of Conduct

Introduction

This code of conduct provides guidance to individuals on how to protect data in the Solita Trusted Research Environment (TRE), constructed and maintained by the Genes and Health study (https://www.genesandhealth.org/) from malicious or accidental threats which may compromise the confidentiality, integrity and availability of data.

The objective of this code of conduct is to provide explicit guidelines for behaviour in support of both the GRL (Sanger) Information Security Policy and the ELGH information security and data protection policies.

Scope

This document must be read, understood and the practices followed by all researchers and system administrators accessing the Genes and Health TRE, regardless of whether they are employed by the Wellcome Sanger Institute or a different organization.

All individuals in scope must attest to following these codes of conduct by emailing genesandhealth@qmul.ac.uk : you will receive instructions on how to submit proof of your Data Security Awareness training, in order to gain access to the Trusted Research Environment.

Codes of Conduct

Cybersecurity Training

All users of the TRE must register at the NHS e-learning for health, and complete the Data Security awareness level 1 course located at :
https://portal.e-lfh.org.uk/Component/Details/544034

Note: when registering for the NHS Learning for Health Site, use ODS Code 8J947 to find Genome Research Limited if you work at Sanger.

Attesting to the code of conduct implies that users have completed this course. Users must refresh their knowledge annually, by retaking the current course.

Password Security

- Passwords must be adequately protected;
- User Passwords must never be written down or stored electronically in clear text, divulged or shared with any individual irrespective of job role or status.
- Users are accountable for all actions associated with their accounts
- All user passwords (Directory Services, Applications etc.) must comply with the following: Initial user passwords must be unique and changed on initial receipt
- Contain a minimum 10 alphanumeric characters
- Be changed when a compromise is suspected
- Not be the same as previously used passwords, or passwords used for other systems/applications

End user devices - Laptops and Desktops

- Individuals are responsible for ensuring their Laptops are adequately protected from Theft or Loss e.g. not leaving devices unattended in areas where there is a risk of compromise
- All newly assigned Mac and Windows devices will only contain user accounts regularly used in the course of their business.
- All newly assigned Mac and Windows devices will have Disk encryption enabled.
- All newly assigned devices will have Endpoint Protection installed (malware detection and exploit protection)
- All Windows and Mac devices have an endpoint firewall enabled (tamper protection in place to prevent removal).
- “Auto-run” or “auto-play” is disabled
- Operating systems and firmware is has security problems regularly fixed
- Internet browser is listed in the user attestation
- Malware protection installed is listed in the user attestation
- Malware software updates reference files daily
- Email application is listed in user attestation
- Unused or unsupported applications are removed
- Operating system updates are applied automatically
- Users are restricted from installing unsigned applications
- Users can only install approved applications

- All users must lock their screens when their device is unattended.
- Device screen savers are enabled following 15 minutes of inactivity for windows devices and 10 minutes of inactivity for Mac devices.
- Use of Removable Media: No Genes and Health data must be stored on removable media.
- Users must not write down or screenshot or photograph or otherwise manually copy sensitive information from the Genes and Health TRE.
- For Sanger staff The 'ICT End User Device Policy' details the Operating Systems (OS) supported by the Institute. All users must cooperate with their organisations to maintain current & appropriately patched OS's.
- Backup of end user device – If enabled by the end user, endpoint devices are backed up to backup software supported and licensed by their organisations.
- Users are not permitted to back up their end user device to other sources.
- Users are not permitted to access the TRE from mobile devices (eg phones)
- As remote working is now very common, all users will *not* use open public networks to access the TRE. Home wifi networks must be secured with strong encryption (WPA2/WPA3). In addition, users will be mindful of their physical location in public environments - e.g. who can see their screen over their shoulder.
- For the AstraZeneca users, the technical and organisational requirements of this section are met by the AstraZeneca Security Policy and the AstraZeneca Corporate Information Technology Usage Standard. AstraZeneca users shall not use any mobile devices to access the TRE. In addition, while connected to the G&H platform AstraZeneca users must lock their screens when leaving their device unattended.

Confidentiality

During or after your participation in the Genes and Health Consortium, you must not disclose any individual level Personal Data or sensitive information from the Genes and Health study.

Consequences of violation of CoC

Users who fail to comply with these requirements will have their access privileges to the Genes and Health TRE revoked.

Reporting a Personal Data Breach

The UK GDPR requires us to notify personal data breaches to the UK data protection regulator, the Information Commission's Office (ICO), and in certain circumstances other regulatory bodies and the data subjects. We have put in place procedures to deal with any suspected personal data breach and will notify data subjects and any applicable regulators where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself or contact the affected data subjects. Immediately contact the Data Protection Team at *hgi@sanger.ac.uk*. You should preserve all evidence related to the potential personal data breach.

If you feel you need to report the breach anonymously, then you can do so via this google form: https://docs.google.com/forms/d/e/1FAIpQLSely3AIVWj2wySAzeJKwfWuIBRtv1VaD9l7Kjnk2jqchb47Ew/viewform

Reporting an Incident

An information security event as defined in ISO 27001:2013, is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.

An information security incident, also as defined in ISO 27001:2013, is defined as single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

All security events and incidents must be reported to GNH Support via one of the following channels:

- Email: hgi@sanger.ac.uk
- The Genes & Health User Helpline Slack channel
- Genes & Health Industry Consortium users can also use the Microsoft Teams channel

- Anonymous reporting via this google form : https://docs.google.com/forms/d/e/1FAIpQLSely3AIVWj2wySAzeJKwfWuIBRtv1VaD9l7Kjnk2jqchb47Ew/viewform

GNH system owners may also directly become aware of an event or incident themselves through security information and event monitoring systems that are in place.

Study partners, patients or organisations within the life sciences industry may also contact GNH to report a perceived security event, incident or security weakness. Any perceived security events, security weaknesses or other incidents reported by customers or business partners must be reported to the GNH Support.

Version Control

Version	Issue Date	Changes	Author
1.0	June 2021	Initial Version	Vivek Iyer
2.0	February 2022	Vivek Amends	Vivek Iyer
3.0	February 2023	Vivek Amends (public environs)	Vivek Iyer
4.0	April 2023	Approved	Vivek Iyer
4.1	March 2024	Annual review	Ben Chewins
5.0	March 2024	Approved	Giles Hamlin
5.1	Feb 2025	Suspension if CoC not followed, revised contact info for attestation , explicit confidentiality clause, security on home wifi networks	Vivek Iyer

Approval

Version	Review Date	Reviewed by
2.0	February 2022	Annual Review
3.0	February 2023	Annual Review
4.0	April 2024	Vivek Iyer
5.0	March 2023	CISO
5.1	April 2023	Vivek Iyer