EXACT SCIENCES

Exact Sciences Privacy and Security Commitment

Exact Sciences recognizes the sensitive nature of health data and the duty to guard its confidentiality. We pledge to maintain the highest level of privacy and security for our patients' trusted information.

Exact Sciences leverages advanced security expertise to safeguard sensitive medical data. We adhere to stringent legal frameworks like Data Processing Agreements (DPA) and Business Associate Agreements (BAA). These compacts are shaped by the mandates of the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA), respectively, ensuring protection through compliance.

Exact Sciences does not sell health information. We collect and use personal data for the singular purpose of performing laboratory tests as permitted by contract.

We utilize administrative, physical, and technical controls to block, identify, and address unauthorized access or breaches. Exact Sciences acts predominantly as a data processor (GDPR) or business associate (HIPAA) and is unwavering in our duty to protect your entrusted data. We infused our data handling practices with features that align with industry norms, meet applicable legal requirements, and best practices to protect patient confidentiality and data integrity.

The following explains how we act to protect the health information you entrust to Exact Sciences.

1. **Purpose** - We only use sensitive health information to conduct laboratory testing services associated with providing healthcare services in accordance with our agreement(s) with our healthcare provider customers.

2. **Minimization –** We practice data pseudonymization and other minimization practices when receiving and using sensitive health information. We only use the personal data necessary to conduct laboratory testing safely and accurately. We follow minimization practices in accordance with privacy regulations such as GDPR and HIPAA.

3. **Transparency** – We understand that it is important to be transparent about collecting, accessing, and utilizing sensitive health information and that it should be lawful and fair. We make all communications related to the processing of personal data accessible and easy to understand, and that clear and plain language be used. Additionally, Exact Sciences complies with individual rights under the GDPR and patient access rights under HIPAA.

4. **Data Isolation** – We do not sell sensitive health information, combine it with other data, or use it for purposes inconsistent with law and contract. Exact Sciences healthcare providers and patients can be assured that the sensitive health information entrusted to us is processed to fulfil our contractual obligations to deliver healthcare services.

5. **Security** – We use strong privacy and security controls to safeguard the personal data entrusted to us.
    a. **Security Culture** – We create a culture of security that begins with our employees. Employees must undergo background checks before joining Exact Sciences. The reference checks, criminal record, credit information, and immigration and security checks. Background checks may differ depending on local laws, regulations, and customs.

    b. **Operational Security** – Consistent with industry best practices, Exact Sciences invests in vulnerability scans, third-party penetration testing, and system/network monitoring. Our security monitoring program focuses on information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. Internal traffic is inspected for suspicious behavior at many points across the Exact Sciences' network. The Information Security team tracks, isolates, and remediates all identified issues.

Data hosted for healthcare is encrypted and isolated in controlled environments as we have implemented many administrative, technical, and physical safeguards (e.g., protect production systems, restrictions on code execution, staged testing and release environments, and monitoring and on-call procedures.

We have a rigorous incident management process for security events affecting systems, data confidentiality, integrity, or availability. If an incident occurs, the security team logs and prioritizes it according to its severity. Events impacting data subjects are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. The Exact Sciences security incident management program is structured around the NIST guidance on handling incidents (NIST SP800–61). To help ensure the swift resolution of security incidents, the Exact Sciences security team is available 24/7 to all employees.

Data Controls Summary

Control	Details
Data Storage	We guarantee US and European data storage regionality for the health information you provide.
Encryption	We encrypt the health information in transit and at rest.
Separation of Duties	We enforce the principle of least privileged access by authenticating all access to data.
Multi-factor Authentication	We use multi-factor authentication (MFA) through technical and physical controls.
Access Monitoring	All Exact Sciences employee end-user access (where applicable) is monitored and logged to enable a complete audit trail.

Prepared by,

Corné Purcell
DPO Exact Sciences