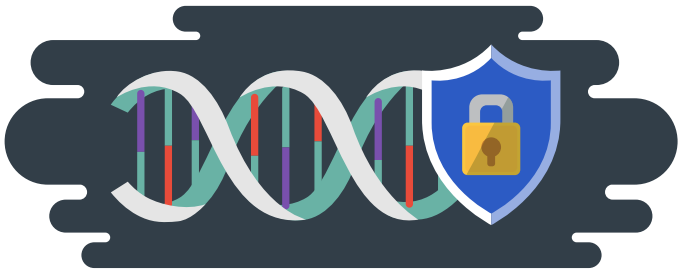
HOW 3X4 PROTECTS GENETIC DATA AND PERSONAL INFORMATION

LAST UPDATED: 27 July 2021

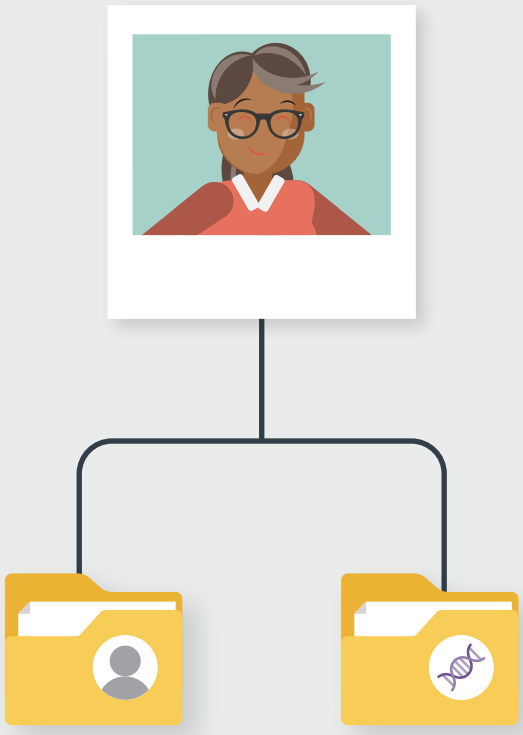
3X4 Genetics understands that health data is highly personal and vital to safeguard. Outlined below are the measures 3X4 takes to ensure that the personal, genetic and health information of our clients is protected and kept private.



Separation of personal and genetic data

3X4 stores personal information (e.g., patient name, contact details, demographic information) and genetic data separate from each other. We use Amazon Web Services (AWS) as our secure cloud storage provider, and these two systems of information are housed in entirely separate accounts. This separation prevents the unintended disclosure of genetic data alongside personal information, and eliminates the danger of genetic data and personal information being associated.

The only time personal information is brought together with genetic information is at the moment the report is downloaded. The PDF report is generated only when a system user (e.g., a practitioner, 3X4 clinician) requests it – it is not stored in that format.



Restricted access to patient data

3X4 limits the number of staff and personnel that can access personal information or genetic data of our patients. The only personnel capable of accessing patient reports, genetic data, or personal information of a patient are:

- The practitioner to whom the patient belongs.
- A limited number of 3X4 staff who require access to this information to support their job function.

We follow best practices with regard to password complexity, and we have strict policies around not sharing credentials.

User activity is logged so that we can trace access and activity.

3X4 GENETICS

Encryption at rest

All data is encrypted at rest (while being stored). This means that any information stored in either of the systems above is stored in a way that ensures that it cannot be read even if the hard disk drives were stolen from the data center. It is automatically decrypted by the systems only when it is needed.

We do not permit any patient data to reside on our staff's work computers. However, they may have emails relating to patient queries. As such, we have a policy that ensures all of our work computers have default encryption enabled, and that our staff secure their profiles with passkeys.

Our email is stored through Office365 Exchange Online, which encrypts the emails for storage.

Encryption in transit

All data is also encrypted when it is being transported between systems. This includes but is not limited to:

Data transfers from the lab to our genetic data system.

Web traffic for users of the 3X4 Portal system, including the download of the generated report.

The data transfer of genetic data during the generation of a report.

Our team uses encrypted transmission technologies for the distribution of sensitive information when our support processes require it.

Regular privacy training and policy updates

All 3X4 staff completes comprehensive privacy training on 3X4 privacy policies and required practices upon joining the company and are required to recomplete this training yearly.

We also regularly send out updates and reminders on best practices and policies to all employees to ensure data security and privacy stays at the forefront of everything we do.