

Privacy

Your patients' information belongs to them. See below for commonly asked questions relating to how we protect your patients' privacy. Additional information can be found at color.com/privacy.

Who will receive information about my patient's test?

Color takes privacy very seriously and complies with HIPAA requirements regarding protected health information (PHI). To that end, Color limits access and disclosure of your patients' PHI to those necessary for the genetic testing and related services. Within Color, the only individuals with access to your patients' PHI are those who need it to provide the Color services. For example, if you or your patient make an appointment to speak with a Color genetic counselor, they will have access to your patients PHI so they can fully discuss questions related to the patient's Color test results. Outside of Color, we provide patients' test reports to the ordering provider, the patient (if they have set up a Color account and the ordering provider has released the reports to them), and to other providers upon a patient's request.

What protections does my patient have against discrimination based upon their results?

The Genetic Information Nondiscrimination Act of 2008 (GINA), the Americans with Disabilities Act (ADA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are federal regulations that safeguard genetic test results and prevent discrimination using genetic information for health insurance and employment status. Some state laws further protect against discrimination in the areas of life insurance, housing and emergency medical services. Federal and state laws regarding genetic discrimination change from time to time. Color encourages you and your patients to keep informed of these important laws and regulations.

Data Security

Security is a primary consideration in everything Color does and the software we build. Our engineers come from top technology companies; they are well-versed in building secure technology.

Is Color HIPAA compliant?

Color follows the applicable privacy, security, and notification rules established in HIPAA, and implements technical safeguards compliant with HIPAA to protect patient data.

What happens in the event there is unauthorized access or use of patient data?

In such an event, Color's internal Incident Response Team would meet to immediately conduct an internal investigation into the root cause and determine whether a reportable breach has occurred as described under applicable law. Based on this investigation, we would implement our Data Incident Response Plan, which includes breach containment, risk mitigation, remediation, documentation, and if necessary, notification. This procedure is designed to meet HIPAA requirements, as well as provide your patients with transparency around our efforts to safeguard their data.

How is patient data protected?

Color uses Amazon Web Service's S3 and RDS services to store our data. At a high level, our data uses anonymized identifiers, and is encrypted at rest and in transit with a modern cipher suite, so this data is only readable by Color. All data access is done using unique identifiers, is logged for auditability, and is restricted only to those Color employees who need access to perform their job duties.

Our security practices have been validated by an independent HIPAA-compliance audit and an independent technical security penetration test. They have also found that Amazon's features allow us to achieve a high standard of data security.

Sample Security

How long will the sample be stored for?

When a patient consents to receive the Color Test, they have the option to store their sample. If the patient has NOT chosen to save their sample, it will be destroyed within 60 days of the test report being generated. If the patient has chosen to store their sample, (1) a saliva sample will be stored for a duration up to Color's discretion; (2) a blood sample will be destroyed within 6 months after a Color test report is generated.

Does Color use the samples for its own or third parties' purposes?

Until such time that a sample is destroyed, Color may de-identify the sample and use it for regulatory compliance purposes; internal quality control; laboratory validation studies; or internal research and development.

When a patient consents to receive the Color Test, they have the option to consent to third party research. Only if a patient selects this option may their sample be used for third party research.

Patients who have previously opted into third party research can opt out at any time by updating their account settings or by notifying the provider who ordered their Color Test. However, if a sample has already been shared prior to such change, Color cannot retrieve the sample.

Questions?

Please contact Color at providers@color.com.

NOTE: This document is for informational purposes only and does not constitute legal advice. Users should consult their own legal counsel for advice regarding the application of the law and this document as it applies to benefits, insurance, and healthcare regulations.