Data security and privacy

5 September 2026 | Version 1.0

Virtual Patient uses fictional patient scenarios to explore physician treatment decisions. Our approach combines data minimisation, controlled project access and human oversight of AI-assisted outputs. Supporting documentation is available for agency security, privacy and supplier reviews.

What data we handle

Patient profiles are fictional research cases, not real patient records. Research data includes treatment choices, physician rationale, drivers and barriers. Limited business contact and access information, such as email addresses, may be needed for authentication and project participation.

Outputs are designed for anonymised or aggregated insight. The respondent identity model and any respondent-level reporting requirements depend on the study setup; fictional patient cases do not mean every item of study data is non-personal.

Real patient records, identifiable patient information and adverse events from actual clinical practice are outside the intended use of the platform. Free-text and spoken responses should relate only to the fictional case. Authorised project administrators can review submitted responses during fieldwork and act under the research organisation's governance and pharmacovigilance procedures if inappropriate information is entered.

Who can access it

Virtual Patient manages application configuration, project setup and access administration. Access is restricted according to project participation and business need, and can be changed or removed when it is no longer required.

Glide provides authentication, row-owner and role-based access capabilities. Project segregation depends on the application configuration and permissions applied to the engagement. Configuration information can be discussed as part of a supplier review.

Hosting and protection

The research application runs on Glide, which provides the managed application platform on Google Cloud Platform. Glide currently identifies Iowa, USA as its server location and publishes information about its subprocessors. Hosting and international data flows should be considered during agency review.

Glide documents encrypted storage and HTTPS connections, and states that it holds SOC 2 Type 2 assurance. This assurance relates to Glide; it is not a Virtual Patient certification. Virtual Patient manages its application and customer workflow, while Glide manages the underlying platform infrastructure and security.

Governance and agency review

AI and human oversight

AI-assisted features can support project setup, fictional patient creation and the synthesis of research findings. AI outputs are working materials for researcher review, rather than authoritative conclusions.

Virtual Patient is a healthcare market research simulation platform, not a clinical decision-support service. It is not intended for diagnosis, prescribing guidance or decisions about real patient care.

AI provider routes, data flows, training-use terms, logging and retention depend on the features and services used. These details should be confirmed for the engagement rather than inferred from a blanket promise about all AI processing.

Retention and incident handling

Project retention and deletion expectations should be agreed for the engagement. Requests concerning account access, relevant personal data or project deletion can be directed to Simon. Glide currently states that deleted platform data is retained for 30 days before permanent deletion; this is separate from the agreed lifetime of an active research project.

Virtual Patient coordinates application-level incident handling and customer communication, involving Glide when platform investigation is needed. The agency remains responsible for its own study governance, respondent consent and regulatory assessments unless otherwise agreed. Notification arrangements and contractual responsibilities should be addressed in the engagement terms.

Supporting your agency's review

A supplier assurance pack is available on request, covering the security and privacy overview, technical and organisational measures, hosting, access, AI governance, retention, incident handling and supporting evidence.

We can discuss supplier questionnaires, data-processing arrangements and information needed for an agency's data protection impact assessment. Project-specific commitments are confirmed through the relevant review and agreement.

Public Glide security documentation is linked below. Restricted assurance reports and testing materials are subject to Glide's controlled access and sharing processes. Virtual Patient can help coordinate the appropriate request.

Sources and contact

Glide Security Center

Glide subprocessors

Glide Trust Center

Simon | simon@virtualpatientapp.com

This public overview describes the intended operating model. It is not a certification, a data-processing agreement or a substitute for study-specific due diligence. Provider statements should be checked against current provider documentation.