redpoint®

The Redpoint® rg1® Approach to HIPAA, HiTrust and SOC 2 Compliance

A Dynata survey on healthcare, commissioned by Redpoint®, reveals a growing preference among healthcare consumers for digital interactions. Consider:

80% **of survey respondents prefer to use digital channels** to communicate with healthcare professionals and brands at least some of the time[1]

44% **prefer digital communications** the majority of the time[1]

65% **have used telehealth services,** and more than one-third of those consumers said they plan to continue to do so[1]

As healthcare professionals and other entities that deal with protected health information (PHI) transition to meet consumer demands for a digital-first healthcare experience, there has been a renewed focus on HIPAA, HiTrust and SOC 2 (Systems and Organizations Controls) compliance, from both a regulatory standpoint as well as to build trust and transparency with the healthcare consumer.

The consequences of failing to protect consumer data make finding a trusted partner an imperative. Consider that in June 2022, the HIPAA Journal reported 70 healthcare data breaches of 500 records or more, well over the 12-month average (57.67). Nearly 6 million healthcare records were compromised, 66% more than the monthly average over the past 12 months. Among them, the Eye Care Leaders ransomware attack affected at least 37 healthcare providers, exposing more than 3 million records.[2]

While HIPAA is legally required for every entity dealing with PHI, and SOC 2 is a voluntary framework (as defined by the American Institute of Certified Public Accountants), privacy and security considerations are central to both.

Redpoint rg1 inherently provides cloud-native (and standards-compliant HIPAA and SOC 2) capabilities for availability, security and governance that are differentiating for healthcare organizations:

- **Keep data in your own security perimeter**
- **Use a PII vault for best practices security**
- **Encryption, hashing, and masking features**
- **Optional data clean rooms**
- **User/role controls for access to the applications and data**

Any healthcare organization that works with PHI must ensure that stringent physical, network and process security measures are in place. A central capability of the Redpoint rg1 environment is keeping all customer data inside the client's own cloud subscription. This is a primary difference between Redpoint and pure SaaS solutions, and allows client IT, compliance and privacy teams to control their data perimeter.

In addition to the inherent security of data-in-place, Redpoint offers a PII Vault as a core capability. The PII vault segregates all PHI into a separate database, with controls for encryption (to prevent interception or visibility of PHI data in the database or in transit), permissions (to control access and usage of individual PHI data) and personalization (to insert PHI data at the moment of usage in a campaign or interaction.

Redpoint also offers operational data clean rooms to allow for the sharing of anonymized data with second parties. Utilizing a type of data encryption that enables organizations to interact with anonymized data without ever accessing or decrypting PHI, the use of a data clean room provides assurances—and transparency—to the healthcare consumer that protecting their data privacy is a top priority.

[1] Consumer Opinions and Preferences About Healthcare Experiences, Redpoint Global Inc. conducted by Dynata, November 2021

[2] June 2022 Healthcare Data Breach Report, HIPAA Journal, Jul 20, 2022

US Headquarters: Wellesley, MA | Tel: +1 781 725 0250 EMEA Headquarters: London, UK | Tel: +44 (0)20 3948 8170
www.redpointglobal.com