



Bishop Fox | Case Study

BUILDING A HEALTHY SECURITY PROGRAM



When Zephyr Health needed help keeping sensitive Patient Health Information secure, they turned to Bishop Fox.

About Zephyr Health Analytics Solution

Zephyr Health helps Life Sciences companies organize and visualize health care data to better connect therapies to patients in need. As an analytics start-up serving the healthcare industry, Zephyr Health needed a solid data security plan and program that they could demonstrate to their clients.

Like many new businesses, they wanted to focus on company security in a more methodical way. And, as a small, but growing company, Zephyr Health needed the ability to accurately answer customer inquiries about their security practices.

Zephyr Health knew about Bishop Fox's strong reputation for helping new businesses secure their networks and applications, but were also eager to learn how we could help in other areas, so that their staff could focus on mission-critical initiatives. We coordinated compliance readiness assessments and implementation services for start-ups like Zephyr as well as Fortune 500 companies.

The Challenge

Zephyr Health approached us to do a policy review and gap analysis against security certifications. Through our consultation process, we determined that the issue was customer-driven.

HIGHLIGHTS

CUSTOMER	Zephyr Health
WEBSITE	zephyrhealth.com
ORGANIZATION TYPE	Healthcare Analytics Software
SERVICES PROVIDED	Policy review and gap analysis against security certifications

- SUMMARY**
- Zephyr Health approached us to do a policy review and gap analysis against security certifications.
 - Our analysis showed that the appropriate security framework for Zephyr Health would be the Service Organization Controls (SOC2).
 - Zephyr Health passed their SOC2 certification within six months with no qualified findings by their external auditors.
 - Customers have reported they feel confident Zephyr Health takes their role as a data custodian seriously.



Scan QR code to access web page



Specifically, Zephyr Health's customers were asking them what they were doing for security, both at a macro (ISO 27001 compliance) and a micro (user authentication) level. We realized they needed to become compliant with a new security standard in order to better develop and maintain their customers' trust.

Our analysis showed that the appropriate security framework for Zephyr Health would be the Service Organization Controls (SOC2), with emphasis on Security and Confidentiality Trust Principles due to several factors, including:

- Small company size
- No prior certification efforts to set precedence
- SaaS-based data analytics services for customers
- The nature of the data they handle (sensitive to their customers, but not relevant for HIPAA or consumer privacy laws)

Zephyr Health's concerns were unique, due to the industries they served. They wanted to not only implement a framework of security management and controls, but also provide peace of mind.

The Result

Bishop Fox worked in partnership with Zephyr Health, providing expertise in customizing the new policy, process, and technical controls to appropriately mitigate the risks to customers. We also implemented new procedures and a proof of control process to protect Zephyr Health and their clients. And, due to the strong relationship between our companies, the transition process moved very quickly.



“Zephyr Health passed their SOC2 certification within six months from start to finish, and with no qualified findings by their external auditors.”

Rob Ragan, Partner, Bishop Fox

Customers have reported they feel confident Zephyr Health takes their role as a data custodian seriously, and can have more strategic conversations about solving their customers' business challenges without security being a cause for concern.

Zephyr Health reports they are now prepared for formally identifying, mitigating and resolving risks to their

environment. This has helped put Zephyr Health clients at ease and enabled them to continue to grow, securely.



“We continue to enjoy the benefits of the SOC2 implementation; thank you again for your help.”

William King, CEO, Zephyr Health

About Bishop Fox

Bishop Fox is a global security consulting firm providing penetration testing, web app assessments, and risk mitigation services to help businesses protect data and assets from cyberattacks. We provide actionable cybersecurity guidance to the Fortune 1000, high-tech start-ups, and financial institutions worldwide.



You can follow Bishop Fox on Twitter @bishopfox.

BISHOP FOX®

Building a Healthy Security Program with Zephyr Health | 05/2018