CUSTOMER STORY

proofpoint.

PROOFPOINT KEEPS CAMARENA HEALTH SAFE FROM PHI EXPOSURE

AUTOMATED PROTECTION GOES A LONG WAY TOWARDS MAINTAINING HIPAA COMPLIANCE

CAMARENA HEALTH

THE CHALLENGE

- Identify PHI and implement strong security policy across network file stores and SharePoint
- Prevent sensitive data from exposure and loss
- Keep up with HIPAA data security compliance requirements and avoid fines

THE SOLUTION

- Email DLP
- Email Encryption
- Data Discover

THE RESULTS

- Automated the discovery of PHI and sensitive data throughout network file shares and SharePoint
- Continuous monitoring automatically identifies and remediates new PHI data
- Gained visibility into emailed documents that contained PHI data violations
- Implemented automated encryption for emails that contain sensitive to prevent data loss

THE ORGANIZATION

Based in Madera, California, Camarena Health began as a single facility with a clear mission: to provide high-quality patient-centered health care for underserved citizens. Almost 40 years later, the community healthcare provider offers high-quality, affordable medical and dental services to nearly 35,000 patients in twelve state-of-the-art facilities.

Like all healthcare organizations, Camarena Health is subject to Health Insurance Portability and Accountability Act (HIPAA) rules. And new healthcare regulations are always emerging. That's why Chief Information Officer Michael Gaskin views compliance as essential.

THE CHALLENGE

Shortly after Gaskin arrived at Camarena Health, he started to rebuild the network and roll out security policies and controls. He was especially concerned about PHI such as patient records and other sensitive data. Under HIPAA, healthcare firms must protect PHI against security threats, loss, and exposure. Most exposure is accidental. People make mistakes. Something as simple as filing a document incorrectly can make a patient record visible when it shouldn't be. Gaskin began researching solutions and weighing his options.

"I spoke with industry peers, and many of them were inclined toward combinations of really convoluted solutions," he said. "I didn't want that. So I did a lot of research online and investigated all of the big names. Then I read some Proofpoint documentation that mentioned a product that scans the network to identify sensitive data, and I was intrigued."

THE SOLUTION

After more research, Gaskin and his IT team chose Proofpoint's Email DLP, Encryption, and Data Discover products. These products classify and protect sensitive data sent via email and discover sensitive data at rest. Email DLP and Encryption work by identifying PHI and other protected data within emails and attachments, and encrypt them automatically. Camarena Health started with Proofpoint's out-of-the-box rules, then customized these to define its own policies. Proofpoint then applied them across the right channels. Employees no longer shouldered the burden of deciding what or when to encrypt their emails.

For files, Data Discover automatically uses the same rules to discover and classify PHI data in network file servers and SharePoint sites. It scans files located across the organization. When Data Discover identifies sensitive information, it automatically remediates any violations.

To identify sensitive data, Proofpoint combines algorithms for detecting Social Security numbers with managed dictionaries specific to healthcare. These

> **"It only takes one file in the wrong place, or sensitive information sent inadvertently to the wrong audience to incur a fine. Proofpoint does exactly what it's supposed to do by locating PHI on our file and SharePoint systems"**
>
> Michael Gaskin, chief information officer, Camarena Health

dictionaries, which are updated regularly, contain common code sets to identify PHI and other health-related information. Code sets include standard disease, drug, treatment, and diagnosis codes.

Email DLP, Encryption, and Data Discover all belong to Proofpoint's Information Protection Suite. Because sensitive data classifiers and policies are consistently shared across this platform, Camarena Health possesses a full-lifecycle approach to protecting PHI.

"Unlike other vendors that have multiple products focused on different things, Proofpoint is straightforward and extremely focused on security," said Gaskin. "Gartner also considers the company to be a leader. It was the combination of being comfortable with Proofpoint as a company and its amazing technology that made the purchase decision easy."

Before Proofpoint, Camarena had no way to find and identify sensitive data at risk, except through manual processes. The task was daunting; Camarena's healthcare records dated back to the mid-1990s.

Data Discover automated scanning of Camarena Health's SharePoint and network file systems to identify PHI. Although Gaskin expected to find many more violations, he was still a bit shocked to see PHI in an operations folder; it could have been easily viewed by anyone.

"I did an initial scan and Data Discover immediately identified PHI in areas where it didn't belong," said Gaskin. "I worked with the health center's Director of Quality to put the files in their proper location."

Dashboard views provide heat maps and excess-exposure charts to help Camarena see where it is most vulnerable. With one click, Gaskin or his team can then drill down to review specific incidents that might require his team to intervene or resolve an issue. Easy-to-use reports summarize:

- Data policy violations
- The number of encrypted messages sent
- The type of content that triggered the encryption or mediation

THE RESULTS

With Proofpoint, communications between Camarena Health and insurance carriers are more secure. Sensitive data in all emails is automatically encrypted based on Camarena Health's policies. That means employees are far less likely to send PHI in unsecured email. And for Camarena, that goes a long way toward preventing data loss.

"It only takes one file in the wrong place, or sensitive information sent inadvertently to the wrong audience to incur a fine," said Gaskin. "Proofpoint does exactly what it's supposed to do by locating PHI on our file and SharePoint systems."

Gaskin plans to continue rolling out more formal data protection and security management policies. He expects Proofpoint to be a key part of that effort. "Proofpoint is a critical pillar of our infrastructure security strategy," he said. "It ensures that PHI is automatically identified and protected by encryption. Now, only authorized staff can see sensitive data. It's just fantastic."

For more information, visit proofpoint.com