

Insurance NetworkingNews

► www.insurancenetworking.com

February 2004, Vol. 7, Issue 7

HealthNow New York

Addresses HIPAA Privacy Issues

By Chuck Paustian

HealthNow New York faced the challenge of protecting sensitive information contained in e-mail communications. By implementing software that allows the carrier to encrypt and monitor e-mails, HealthNow New York is complying with HIPAA privacy regulations while serving its customers.

Imagine if your company's e-mail — that ubiquitous business tool for conveying information in a near instantaneous and inexpensive manner — was removed from your organization's communication options.

That's the scenario that health insurers, health plans, providers and other organizations faced when the privacy rules of the Health Insurance Portability and Accountability Act (HIPAA) took effect April 14, 2003. Under the provisions of the federal legislation, the confidentiality of sensitive data, such as personal health information, had to be protected. Because the Internet is an open network, health care organizations either had to find a way to protect the information conveyed in e-mails or rely on less efficient communication channels, such as faxes or the postal service.

"We told people that if they were

sending sensitive information, they could no longer do so through e-mail," said Nancy L. Schoellkopf, corporate HIPAA privacy official for HealthNow New York Inc., the Buffalo, New York-based parent company of BlueShield of Northeastern New York and BlueCross BlueShield of Western New York. However, that would hinder tremendously HealthNow's ability to communicate with its more than 900,000 members in 53 New York counties and process the 850,000 claims it handles in an average month.

"We were aware of the possibility that sending sensitive information via e-mail would be a problem," said Schoellkopf. "But, we were getting questions from our workforce about whether it was okay to send certain information via e-mail."

So, rather than rely on faxes and the mail, HealthNow executives decided to find a way to continue to use e-mail. The

solution would have to meet three objectives — total encryption of outgoing e-mail, a monitoring system to ensure compliance with corporate policies and other regulations such as HIPAA and facilitation of communication.

A total of five vendor systems were evaluated, but four were eliminated for various reasons. In the end, HealthNow hired Zix Corp., a Dallas-based provider of e-messaging protection and transaction services, to implement the Zix VPM software for scanning and encrypting e-mail messages.

"As we went through the evaluation process ... whenever we had a question or concern Zix worked very closely with us to make sure we had an appropriate response," said Sean Kelly, information security analyst for HealthNow. "As with anything, you want to have that good working relationship."

The Zix solution includes a content

scanning lexicon for HIPAA-related terms as well as a customized lexicon for company-specific information such as member and policy numbers. Outbound e-mails are scanned and all sensitive information is encrypted. For the HealthNow plans, the intended recipient is directed to one of three portals, all branded and customized, where they can receive their e-mail and respond if necessary.

Although all outbound e-mails are scanned, HealthNow departments generating e-mails that contain sensitive information are required to include keywords in subject that trigger the scanning and encryption process.

Each day the Zix system generates a report that shows which e-mails were encrypted. "I'm really happy with the daily logs. I get the logs in the morning and spend about five minutes going through them," Kelly said. "That really gives us a lot of flexibility to make sure we're in compliance with our policies, HIPAA and everything else."

Schoellkopf said the Zix system was

installed with relatively little disruption to business. She said HealthNow executives spent about a half of a day with Zix representatives to discuss changes to the company's existing technology infrastructure. The actual installation only took one day. HealthNow tested the system for several weeks to ensure it was working properly before going live.

To facilitate the implementation process, HealthNow distributed information on the new system through its intranet and its quarterly member newsletter. "There was no extra training required other than those few communications that we sent out," said Kelly. He added that he made sure a lot of key people, including senior executives, were involved in the project from the beginning and that also helped the transition process.

Schoellkopf said the Zix system has more than met expectations. "We've been very pleased with everything," she said, adding that there were some unexpected benefits, such as the ability

to append a disclaimer to outgoing messages. "Those little bonuses are very nice and are pleasant surprises."

As a result, HealthNow is considering another Zix product that would allow health care providers to send information to the company via encrypted e-mail. "That's something we may look at down the road," Kelly said. "It would be good for providers to be able to send us e-mail in that way."

While it's virtually impossible to determine a return on investment for the scanning and encryption system, Schoellkopf said the money was well spent. "It's definitely a significant investment from our perspective and with these types of security products, there's really no return on investment," she said. "But, part of our payback is that we're protecting our members sensitive information."

And that carries very real, if immeasurable, benefits, added Kelly. "We feel a member would view it as a positive thing that we're trying to protect their information," he said. ■



2711 N. Haskell Ave. Suite 2300, LB 36 Dallas, TX 75204-2960
Tel: (866) 257-4949 • sales@zixcorp.com • www.zixcorp.com