



ZixGateway® Inbound

Protecting patient data

Benefits:

- Proactively identifies inbound email PHI breaches
- Inbound HIPAA content scanning
- Quick deployment in less than a day
- No software to install and no additional resources needed
- Seamless integration with existing infrastructure and systems

Features:

- Policy management for HIPAA compliance
- Full content scanning of message and attachments
- Automated breach notifications
- Daily policy breach reports

The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA), calls for protected health information (PHI) to be rendered unreadable and unusable. Under the new legislation, organizations can be fined up to \$1.5 million for violating the rules protecting patient privacy. Their business associates are also covered as part of the most recent changes.

For many healthcare organizations, safeguarding email sent by its employees is not enough. They also want to proactively identify any potential vulnerabilities. ZixCorp® Email Encryption Services are an important solution in the protection of sensitive data, and now ZixGateway Inbound provides a way for healthcare organizations to better manage your HIPAA compliance.

ZixGateway Inbound monitors email communication and notifies you when an email contains unprotected PHI. With full content scanning of your inbound email, ZixGateway Inbound enables you to better manage your HIPAA compliance.

Automated compliance management

With ZixGateway Inbound, inbound email is content-scanned for unsecure PHI. When vulnerabilities are identified, both the business associate and the appropriate internal compliance manager can be automatically notified. This enables healthcare organizations to proactively identify vulnerabilities, as well as protect their patients and their brand.

Proven HIPAA lexicons

Using the same industry-proven, healthcare lexicons as our standard ZixGateway policy-based email encryption solution, ZixGateway Inbound identifies sensitive PHI in both the email message and attachments. The lexicons search for PHI by taking the intersection of identifying information, as set forth by the Department of Health and Human Services, and health terms or claims information. This provides the highest level of assurance that unencrypted PHI is identified and your organization can take action.

About Send Privately

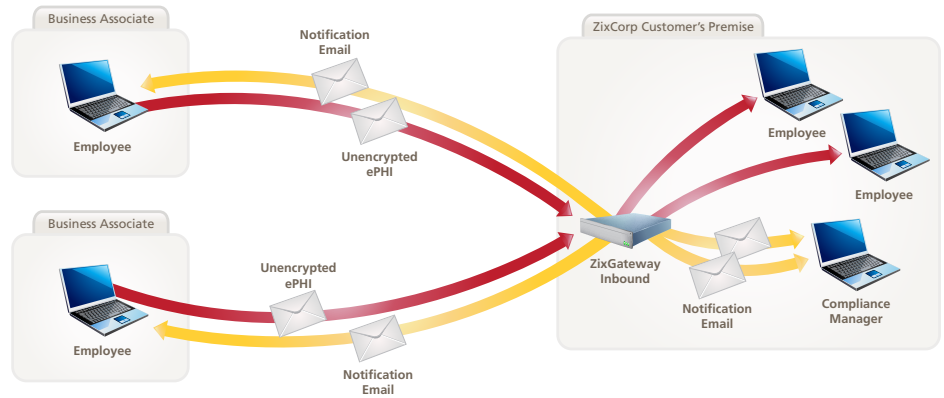
Send Privately is a brand of Seacoast Telecommunications Service Bureau, Inc., a Manage Service Provider (MSP) since 1995 with more than 5,000 customers in over 100 countries.

Seacoast Telecom is rated high in customer care and technical support and offers high-quality managed hosted services and in-house developed solutions at the industry forefront, including: Hosting Solutions; Cloud Hosting; and Email and Collaborative Applications.

Strategic partnerships with industry-recognizable leaders include ZixCorp; Parallels; Google; Microsoft; and other leading technologies.

Our ZixCorp partnership combines the dedicated email encryption experience of market-leader ZixCorp with our expertise in product implementation, application management, and customer service skills.

Such unique experience earned Seacoast Telecom the highest partner-level status as a ZixCorp Diamond Managed Service Provider and the highest partner-level status with Microsoft and Parallels.



Policy enforcement with ZixPort®

ZixPort is a secure portal that enables healthcare organizations to provide bi-directional secure communication at no cost to business associates. In addition to providing an easy-to-use, custom secure portal for business associates to read and reply to encrypted email, ZixPort allows the business associate to initiate a secure email to the healthcare organization. Healthcare providers can provide a link from their Web site to the secure portal and then use ZixGateway Inbound to ensure business associates are using it to properly secure PHI.

HIPAA compliance reporting

ZixGateway Inbound provides thorough reports that log the details of inbound vulnerabilities. The reports can be sent to the compliance or security staff on a daily basis for additional review and action. Taking proactive steps to monitor inbound communication, in addition to encrypting your outbound communication, will greatly reduce the risk of disclosing patient information.

Send Privately
10 Second Street
Dover, NH 03820

Phone 888 509 8555
SendPrivately@link2exchange.com
www.sendprivately.com