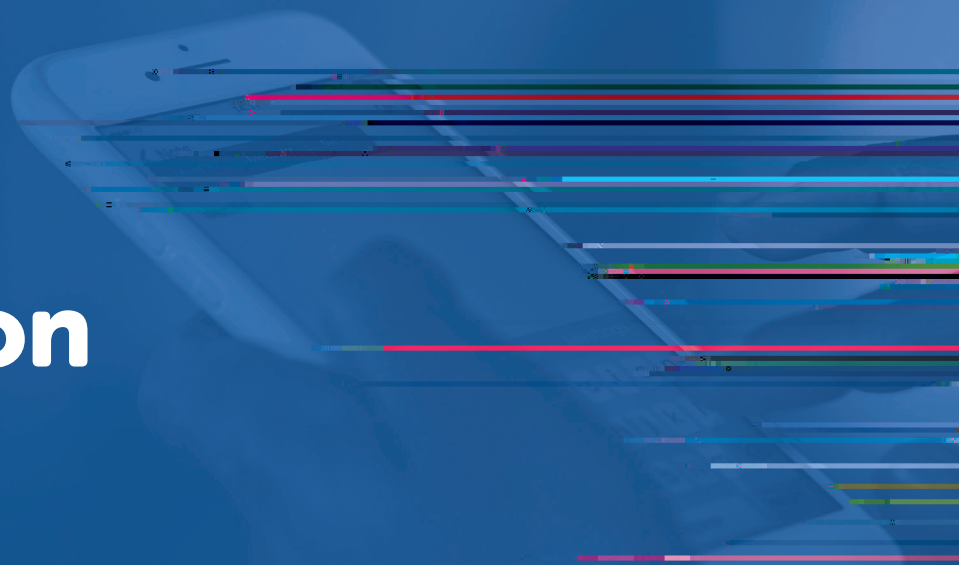
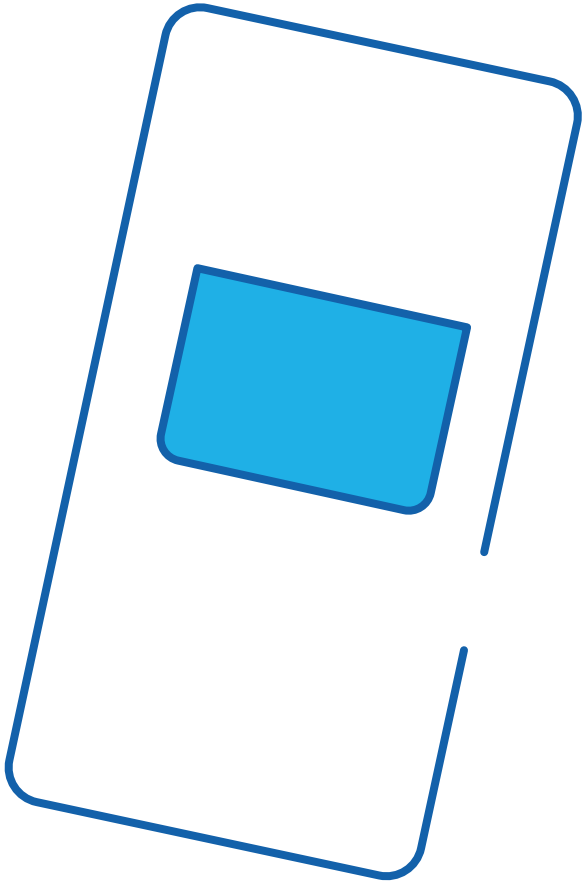
/ CASE STUDY

Memorial Hermann Health System Eases Email Encryption with Zix

Learn how Memorial Hermann uses ZixEncrypt to easily secure protected health information and other sensitive data





Automation Enables Protection and Compliance

Just as encrypted email is convenient to receive, it is also convenient to send. With out-of-the-box automatic policies for Health Insurance Portability and Accountability Act (HIPAA), Social Security numbers and financial information, Memorial Hermann has confidence that emails with sensitive information in the message or attachment are protected. When a policy is triggered, emails can be encrypted, blocked or quarantined depending on the content, sender or recipient or other policies.

"Zix email encryption and policies are a way for us to meet our HIPAA requirements and automatically prevent spillage for everyone in our organization. It serves as a cost saving measure, keeping us from facing fines related to a breach," said Santiano .

HIPAA requires that protected health information (PHI) be "unusable, unreadable or indecipherable" to unauthorized individuals. More than 1,200 U.S. hospitals trust ZixEncrypt to assist with their compliance when exchanging PHI in email.