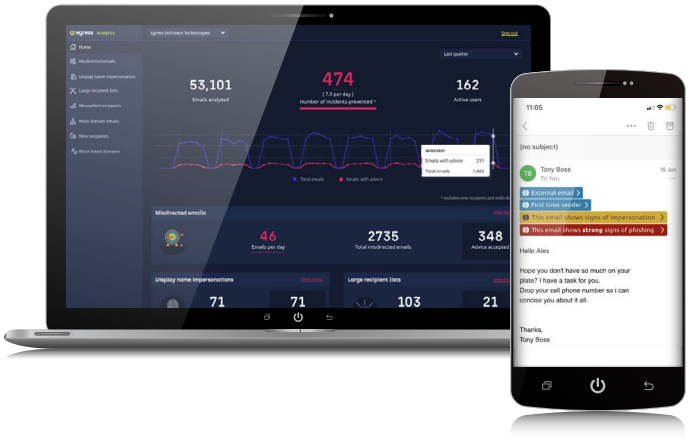
egress

HIPAA compliant email in a box

Keep protected health information secure and avoid financial penalties with our **all-in-one intelligent email security platform**

The consequences of violating the Health Insurance Portability and Accountability Act (HIPAA), either wilfully or accidentally, can be severe. Financial penalties, unwanted litigation costs and reputational damage, not to mention criminal charges, potentially await companies and individuals who fail to comply. And with over 75% of CISOs in healthcare saying that employees regularly put sensitive email data at risk, a robust safety net is needed.

We provide a far-reaching email security solution that helps covered entities safeguard electronic Protected Health Information (ePHI), remain HIPAA-compliant and, importantly, avoid financial and reputational damage.



Prevent an email security breach

Minimize the threat of a HIPAA violation.

Keep sensitive data safe

Avoid unauthorized access to sensitive data.

Stop zero-day phishing attacks

Detect and mitigate target inbound email cyberattacks.

Avoid financial and reputational loss

Stay clear of fines and litigation by remaining compliant.

Intelligent email security: HIPAA email compliance in a box

Our Intelligent email security platform is an all-in-one solution that removes the risk of an email security breach and keeps personal health information safe.

Egress Defend combines zero trust with natural language processing and machine learning to detect and mitigate all targeted inbound phishing attacks. **Egress Prevent** utilizes contextual machine learning to deeply understand a user's working patterns, spot abnormal behavior, and prevent emails going to the wrong recipient or with the wrong content. **Egress Protect** makes sure that users send sensitive email content with the appropriate level of encryption.

Securing **1,000+** large organizations

Top five features

Visit **www.egress.com** for more features

1. Contextual machine learning
2. Natural language processing
3. DLP policies and scanning
4. AES 256-bit encryption in transit and at rest
5. Available on all mobile devices

Supporting HIPAA compliance

Section	Requirements	How we help
45 CFR § 164.306(a)(2)	**Protection against cyber threats** Covered entities and business associates must protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.	**Egress Defend** uses zero trust models, machine learning and natural language processing to detect targeted and sophisticated inbound email attacks, including business email compromise, supply chain compromise and impersonation attempts. This includes weaponized attachments and URLs (including hyperlinks that are activated post-delivery). The technology also provides real-time teachable moments that quickly and easily explain cyber risk to rushed healthcare workers, empowering them to become cybersecurity assets that can better detect and mitigate future threats.
45 CFR § 164	**Impermissible disclosure** Entities cannot share ePHI with a third party, wilfully or by mistake, without a patient's prior consent.	**Egress Prevent** eliminates the risk of impermissible disclosure by using contextual machine learning with DLP policies to analyze user sending patterns, spot anomalies and prevent emails being sent to the wrong recipient or with the wrong content. We interrogate an email's subject line, message body, attachment name and type, and data inside an attachment to make sure the email content goes to the right person and prevents a security breach.
45 CFR § 164.312(e)2	**Use of encryption** Organizations must implement encryption to NIST standards if, after a risk assessment, they determine that it is reasonable and appropriate to safeguard the confidentiality, integrity and availability of ePHI.	**Egress Protect** enables employees to keep sensitive data safe by manually applying the appropriate level of security to sensitive emails, while granular permissions such as read only access and restricted forwarding remove the risk of unauthorized viewing. **Egress Prevent** eliminates the risk of a security breach by using DLP scanning on emails to intelligently recommend, or even enforce, encryption when risk levels are high.

For more information please contact your account manager or call 1-800-732-0746

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

CESG Certified Product Foundation Grade DGEE378428688-1104 · bsi. ISO/IEC 27001 Information Security Management · Common Criteria · NATO OTAN

www.egress.com | info@egress.com | 1-800-732-0746 | @EgressSoftware