Governance IT®

Governance,
Risk and Compliance
Consultancy
for eCommunications

Compliant eCommunications for Life Sciences

Express Gap Analysis

eMail in the context of Risk Management

In **21%** of all court cases eMail is used as evidence.

13% of company's are engaged with court cases attributable to content in employee eMail.

65% of all companies have no eMail (retention) policy.

94% of all companies fail to archive Instant Messages

46% of all companies have no policies around electronic communication nor education on these.

50% of all users either send or receive electronic communication with high risk content in the form of file attachments, jokes, rumours, confidential information or porn.

GOVERNANCE IT is a company specialising in the delivery of compliant eCommunications consultancy. We guarantee you 100% updated knowledge on all rules and regulations regarding eCommunications.

Overview

Express eCommunications Gap Analysis

HIPAA Requirements

Roadmap to eCommunications Compliance

Information Management & Business Controls for eMail

eCommunications Analysis for Life Sciences Companies

eMail and Instant Messenger are technologies without which it is hard to imagine business being conducted - but it is a convenience which brings with it a security risk.

Developing a framework for the secure and efficient management and distribution of company information and in particular non-public information (NPI) is a complex and time consuming task— and one which makes no consideration for size of company.

At Governance IT we focus exclusively in the deployment of standardised best practices for the management of electronic communications. Using industry specific templates we ensure that you live up to whatever demands your management or regulatory bodies may have.

Often the first problem is understanding where you are and where you want to be - and this is where Governance IT's **Electronic Communications Gap Analysis** comes in and gives your company the following:

- Brief view over the rules and regulatory requirements specific to your company
- Which rules are currently covered by your company's policies, procedures and control points?
- Which rules are currently not covered by your company's policies, procedures and control points?
- Recommendations to key changes and processes to ensure basic compliance.

Contact Frederik Fabricius on +45 7026 0350 and book a meeting to discuss.

Healthcare Security & Privacy

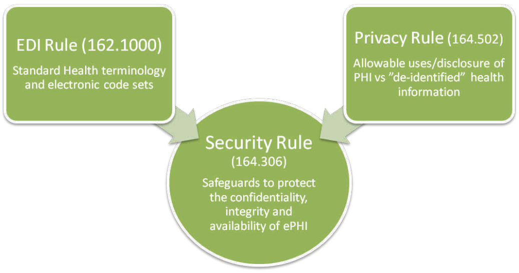
A Healthcare Privacy Solution helps organizations assess risk and comply with the HIPAA Security Rule, which defines guidelines and standards to safeguard ePHI or other company sensitive information.

At the heart of any risk assessment a company needs to be secure in the knowledge that all electronic communication in the form of eMail and Instant Messenger is managed and that rules can be enforced.

HIPAA laws and ISO standards provide a useful framework for identifying key safeguards - whether they be administrative, physical, organizational or procedural - for defining a complete information security management system.

At Governance IT we base our best practices on HIPAA Rule 164.306/308/310/312 and the ISO 27001 Information Security Management System framework. Our roles-based approach and pre-populated industry-specific templates ensure an efficient and swift deployment.

The Governance IT Express Gap Analysis for electronic communication provides the foundation for mapping your current state and risk exposure and a roadmap to implementing compliant and secure information management.



EDI Rule (162.1000)
Standard Health terminology and electronic code sets

Privacy Rule (164.502)
Allowable uses/disclosure of PHI vs "de-identified" health information

Security Rule (164.306)
Safeguards to protect the confidentiality, integrity and availability of ePHI

Governance IT®

Performing an electronic communications risk assessment

Forrester Consulting found that more than 70 percent of large companies polled were concerned or very concerned about leaks of valuable intellectual property and trade secrets via email.

Irrespective of which levels of compliance your company faces there is always a requirement to manage the company's non public information (NPI), whether they be patient information, financial information or valuable intellectual property.

The Governance IT Express eCommunications Risk Assessment takes it's starting point in key elements as defined by HIPAA and ISO 27001.

Islandsbrygge 43
DK 2300 Copenhagen
Tel: +45 7026 0350

www.governance-it.com

eCommunications Security and Risk Management

Compliance strategies and best practices

Best practices in compliance dictate how employees must deal with various tasks and business processes, in line with industry specific demands.

Information security management

Information security management incorporating regulatory compliance, risk management, information security standards, security frameworks, disaster recovery and more.

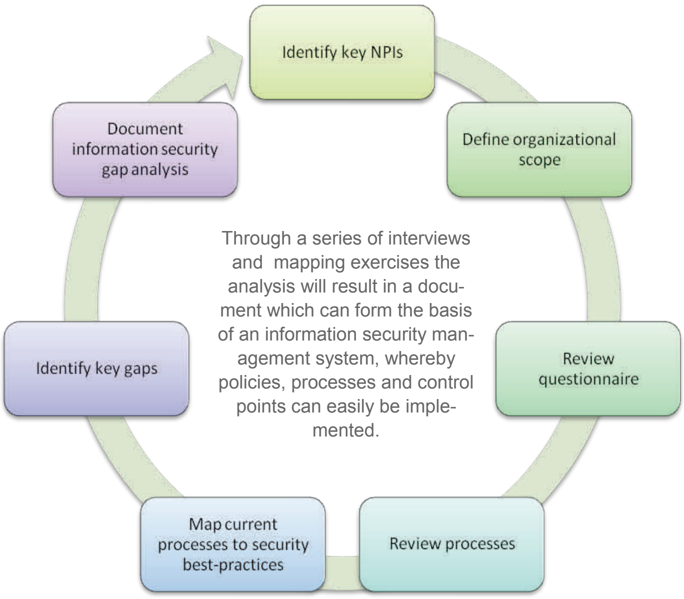
Risk management

An effective risk management plan includes ways an IT department can help minimize the effects of risk of an organization's assets and data.

Data security and privacy

Efficient use of technology to share data whilst still following specific rules and regulations to protect non-public information.

Ask about our 30 Day
Data Leakage
Assessment Report



Identify key NPIs

Define organizational scope

Review questionnaire

Review processes

Map current processes to security best-practices

Identify key gaps

Document information security gap analysis

Through a series of interviews and mapping exercises the analysis will result in a document which can form the basis of an information security management system, whereby policies, processes and control points can easily be implemented.

Security Assessment for Electronic Communications

Sample Assessment	
Security Management Process § 164.308 (a)(1) (i) – (ii) (D)	Have you implemented policies to prevent, detect, contain and correct security violations? Do you have a sanction policy in place to apply sanctions to staff that fail to follow your security policies and procedures?
Workforce Security § 164.308 (a) (3) (i) - (ii) (C)	Have you implemented a policy to ensure all staff has appropriate access to NPI and to prevent those who do not from obtaining access to NPI?
Information Access Management § 164.308 (a) (4) (i) – (ii) (C)	Do you have a policy for authorizing access to NPI? Have you addressed policies for granting access to NPI (e.g. through access to a workstation, transaction, program, or process)? Have you implemented a policy based on access authorization policies, establish, document, review, and modify a user's right of access (to a workstation, transaction, or program, for example)?
Security Incident Procedures § 164.308 (a) (6) (i) - (ii)	Do you have a policy that addresses identifying and responding to suspected or known security incidents, mitigating the incident, and documentation of security incidents and their outcomes
Contingency Plan § 164.308 (a) (7) (i) – (ii) (E)	Have you implemented a policy for responding to an emergency or other occurrence that damages systems that contain NPI?
Access Control § 164.312 (a) (1) – (2) (iv)	Do you have a technical policy for systems that maintain NPI to allow access to only those persons or software programs that have been granted access rights?
Integrity § 164.312 (c) (1) – (2)	Do you have policies to protect NPI from improper alteration or destruction?
Security Awareness Training § 164.308(a)(5)(i) – (ii)(D)	Have you implemented a security awareness program for all staff (including management)?

Governance IT partners: CONTROLLERS proofpoint netIQ An Attachmate Business Built on IBM express advantage offerings