

Overall objective: Determine if email systems and policy have the ability to provide confidential email communication to its partners and employees, to protect its employees and organization from potential legal liability, to ensure privacy and integrity of patient, clinical data, and other sensitive information transmitted via email, and to mitigate the risk of compromising the organization’s data and systems as a result of email communication.

Audit Steps	WP Ref.	Prepared By
<p>EMAIL POLICY –CONFIDENTIALITY and PRIVACY</p> <p>1.Determine if there is an approved corporate email policy and if the policy stipulations mitigate the organization’s exposure in the event of liability claims. Assess whether the policy clearly addresses the following issues:</p> <p>1.1 Email systems are the employer’s <u>not</u> the employee’s property and the organization has the ability and right to retrieve, review, audit, intercept, access, and disclose any messages sent or received via email.</p> <p>1.2 Only authorized personnel may inspect and monitor electronic communications.</p> <p>1.3 Email communication is to be used primarily for business purposes, where ‘primary’ is defined depending on the business culture.</p> <p>1.4 Monitoring software may be used to enforce policies and filtering software may be used to filter email content (e.g., Spam).</p> <p>1.5 Email, as any other software, should not be used as a vehicle to disseminate unauthorized proprietary data, disseminate or download unauthorized materials from the Internet, including unauthorized anti-virus or anti-copyright infringement software.</p> <p>1.6 Spells out whether employees are allowed to use the corporate network to access personal web-based email, restricted, not at all, or occasional and incidental.</p> <p>1.7 The Internet policy is integrated with the email policy and is meant to help employees understand that outbound email communication via the Internet is not secure even if it is encrypted and that viruses can be introduced on internal networks through web-based mail, such as Hotmail, Yahoo, or Zdnet.</p> <p>1.8 The policy should define when and when not to encrypt email. Determine if the policy raises awareness among users regarding the inability of the email systems to verify the identity of the sender and the integrity of the message.</p> <p>1.9 Misuse of systems will result in disciplinary action up to and including termination.</p> <p>1.10 Prohibits disseminating chain letters or literature that use valuable network resources and can lead to email system unavailability or may include political statements.</p> <p>1.11 Prohibits posting or downloading pornographic material.</p> <p>1.12 Prohibits communication of discriminatory remarks regarding sex, gender, age, religion, national origin, marital status, height, race, or minorities or other groups protected under the equal employment opportunity laws.</p> <p>1.13 Prohibits the use of sexually explicit, obscene, harassing, inflammatory or offensive language, or that violate the company’s equal opportunity or sexual harassment policy.</p> <p>1.14 Prohibits communication that may promote or comprise a criminal offense.</p> <p>1.15 Prohibits the use of threatening, reckless, or ‘maliciously false’ content.</p> <p>1.16 Prohibits use of email to further a personal business activity exterior to the company’s objectives.</p>		

Audit Steps	WP Ref.	Prepared By
<p>1.17 Prohibits use of email to conduct membership drives, solicit funds, or sell services or products, unless explicit permission is provided by senior management.</p> <p>1.18 Prohibits the use of email to engage in computer hacking and related activities.</p> <p>1.19 Prohibits the use of email to access codes or unauthorized data.</p> <p>1.20 Prohibits the use of email to attempt to disable or compromise security of data stored in company's systems.</p> <p>1.21 Prohibits altering default email system settings without approval.</p> <p>1.22 Prohibits other inappropriate use of email systems.</p> <p>1.23 Emphasizes that employees should carefully compose email messages, avoiding ambiguity and slang that may lead to misconstrued interpretations.</p> <p>1.24 Recommends the use of disclaimers for raising employee's awareness of email policies, indicating that the email content does not represent the official view of the company.</p> <p>1.25 Addresses implementation and configuration of anti-virus software and firewalls on all servers and clients, including privately owned desktops and laptops that are not owned by the enterprise, but are used by remote users or those who transfer files between work and home, to conduct enterprise off the premises, whether via diskette, or email.</p> <p>1.26 Requires users to scan a CD, diskette, local hard drive, and files downloaded from remote sites.</p> <p>1.27 Spells out consequences of non-compliance.</p> <p>Risk: a policy with incorrect or insufficient stipulations and restrictions may result in corporate liability, company may not be able to safeguard employees from discrimination and harassment, intellectual property violation, such as software piracy, compromise the overall company legal and ethical standards. thus incurring litigation costs and substantial damages.</p>		
<p>2. Determine if the policy is adequately written and implemented, as well as it is aligned with the organization's long-term goals.</p> <p>2.1 The policy is clear, concise, easy-to-read and understand.</p> <p>2.2 The policy was developed with involvement from IT, human resources, legal departments; was formally approved and signed-off by senior management.</p> <p>2.3 The policy was established based on a risk assessment and needs-based, strategic cost-benefit analysis to take into account variables privacy, confidentiality, non-repudiation, and integrity of email.</p> <p>2.4 Review the IT's strategic plan to identify long-term strategies for email policy and infrastructure deployment. If no such information exists, obtain long-term strategy guidelines from management. Assess if the strategy includes variables such as: ease of use, deployment, and maintenance, user community breath and depth, end-to-end confidentiality and integrity, mutual authentication of identity of receiver and sender, non-repudiation of origin, auditability of email message receipt, integration with existing security infrastructure, ability of the user to control email sent, etc.</p> <p>2.5 The email policy is distributed in conjunction with an overall security awareness plan that includes user training so that users know what risks are being addressed by the policy.</p> <p>2.6 Employees are aware of the existence of such policies. Test for a sample of IT managers (via questionnaire).</p> <p>2.7 There is a process in place to make policy changes.</p>		

Audit Steps	WP Ref.	Prepared By
<p>2.8 The email and Internet use policies are strongly integrated and account for email being the most prevalent computer virus infection mechanism. Determine if management has considered a decision should be made as to blocking web-based mail sites, such as Yahoo and Hotmail, which allow employees to check web-based email while at work, from machines connected to the organization's networks.</p> <p>Risk: A policy not implemented correctly has no effectiveness.</p>		
<p>3. Determine if the policy accounts for archival, storage, and periodic destruction.</p> <p>3.1 Determine if there are email recording and archiving capabilities and if there is an established mail document retention period in the policy.</p> <p>3.2 Determine if this retention period was established based on decisions made by business area management and legal department based on business risks assessments and regulatory, contractual, or external control requirements.</p> <p>3.3 Determine if servers have the capability to store messages. If messages are stored, determine if logs are protected against unauthorized access and manipulation. (Conversely, the email systems have encryption and key escrow that effectively expire email effectively whenever messages have been sent.)</p> <p>Risk: lack of electronic trail may hinder the organization from withstanding legal scrutiny related to contractually obligating electronic messages; if email is subpoenaed, the company can incur significant costs in searching huge tape backups. Emails can be stored on servers, client machines, and printed. An effort to provide email evidence as a result of a subpoena in an environment that lacks policies for archival and retention can be cost prohibitive and bring IT services to a halt. This represents a higher risk than actual clear-text transmission. In our environment, email is used as a file transfer vehicle and means to exchange patient information.</p>		
<p>4. Determine if the policy and changes to policy are communicated to employees effectively, clearly, and thoroughly. Assess the following elements in relation to the email policy:</p> <p>4.1 Is the policy communicated through orientation, educational sessions, meetings, briefings, presentations, open houses, policy awareness days, regular breakfasts, lunches followed by Q&amp;A sessions, open-door policy for email policy related inquiries, voice mail reminders, information sessions via video or computer conferencing, other activities?</p> <p>4.2 Is the policy communicated via printed materials, e.g., posters, newsletters, fact sheets, brochures, FAQ sheets, desk calendars, mouse pads, postcards, memoranda, letters from executive management, policy outline in the employee handbook.</p> <p>4.3 Are employees asked to acknowledge their understanding of policies in writing to reinforce the policy?</p> <p>4.4 Are hardcopy documents posted and distributed to employees to enforce policy?</p> <p>4.5 Are timely reminders extended to employees in addition to the policy manual? Assess frequency.</p> <p>4.6 Are employee history reports or an electronic paper trail, such as a database, for use in the event of a violation or court action? If yes, is this database secured from unauthorized access?</p> <p>4.7 Is there a process to track employees' responses and address concerns before they escalate into problems?</p> <p>4.8 Are physicians and other medical care personnel advised of Electronic Patient Care Communication guidelines regarding confidentiality, integrity, availability of email communication.</p> <p>Risk: corporate liability from non-compliance with rules and regulations; lack of effectiveness if no approval from executive management), may not protect employees from discrimination and harassment, may lower employee productivity due to personal email.</p>		
<p>EMAIL USER TRAINING AND AWARENESS</p> <p>5. Determine what type of action is taken by IS to train users about:</p> <p>a. Email policy enforcement.</p>		

Audit Steps	WP Ref.	Prepared By
<ul style="list-style-type: none"> <li>b. Email risks and vulnerabilities.</li> <li>c. New types of viruses.</li> <li>d. Action to be taken when an infected file is found.</li> <li>e. How to scan a CD, diskette, local hard drive, and files downloaded from remote sites.</li> <li>f. Social engineering and how email users can be tricked into releasing critical security information.</li> </ul>		
<p>6. Determine if robust information security practices are used to address the growing threat of security breaches associated with email use. Assess the following controls:</p> <p>6.1 The organization has written, periodically reviewed, and updated email standards that are mandated across the organization.</p> <p>6.2 There is a corporate-level staff function dedicated to maintaining and enforcing email security standards.</p> <p>6.3 All known instances of noncompliance with information security standards are documented and reported regularly to senior management.</p> <p>6.4 Determine if the policy, standards, or best practices define the type of servers (e.g., at a minimum all file servers) that need to have anti-virus software implemented, implementation and configuration of anti-virus software, the type of files or attachments to be scanned, action to be taken if an infected file is found, etc.</p> <p>Risk: hacks, negligence, misuse, and abuse of email systems resulting in theft or inadequate disclosure of sensitive information. Widespread distribution of email systems across network email servers and outside the network, personal desktops in and outside the office. This creates a high number of potential targets for attackers. One security failure within an obscure email client or server could compromise the whole system. The effectiveness of firewalls or VPN is limited.</p>		
<p>7. Validate that the email policy is in compliance with applicable rules and regulations.</p> <p>7.1 Via inquiry with Legal, HR/Benefits, Compliance, Security, Finance/Controller's departments, obtain an understanding of applicable federal and state rules and regulations that may impact the use of email. Compile a listing of such regulations and discuss it with the in-charge manager.</p> <p>7.2 Using a spreadsheet format, document the following fields: rule/regulation name, brief description, potential email implications, desired controls, and implemented controls.</p> <p>7.3 Use the spreadsheet developed in 7.2 to compare controls identified in audit step 1, fill in the 'implemented control' column</p>		