AFFILIATED PHYSICIANS
ON-SITE VACCINATION AND WELLNESS SERVICES

HIPAA Core Policy: Internet and Email Use

Abstract:
This policy sets forth rules for the use of email and internet so that such activity does not negatively impact the confidentiality, availability, integrity, and reputation of AFFILIATED PHYSICIANS and their assets and supports applicable federal and state laws.

Effective Date:
03-19-21
Responsible Party:
Steve Naidich
Applies To:
All Internal and Contracted Employees

1. PURPOSE: To ensure that the use of email and internet activities do not negatively impact the confidentiality, availability, integrity, and reputation of AFFILIATED PHYSICIANS and AFFILIATED PHYSICIANS Health System and their assets and to ensure compliance with applicable federal and state laws.

2. PHILOSOPHY: An authorized user's access to the Internet and/or email services for limited personal use is a privilege that, if not properly monitored and controlled, could result in harm to the organization or violations of certain federal and state laws. The primary use of these services is for business and clinical purposes and thus need be appropriately protected.

3. APPLICABILTY: This standard applies to all AFFILIATED PHYSICIANS

4. DEFINITIONS:

4.1. ***Protected Health Information (PHI)***: Health information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium. PHI does not include individually identifiable health information in patient records covered and protected by Privacy Act and employment records held by a covered entity in its role as an employer.

4.2. ***Sensitive Information or Data***: Data that should be kept confidential. Access to these data shall require authorization and legitimate need-to-know. It includes Protected Health Information, financial information, personnel data, trade secrets, and any information that is deemed confidential or that would negatively affect AFFILIATED PHYSICIANS if inappropriately handled.

4.3. ***Email***: The electronic transmission of information through a mail protocol such as SMTP, POP, or IMAP.

5. POLICIES:

5.1. All email messages, documents, and correspondence and data obtained through AFFILIATED PHYSICIANS or AFFILIATED PHYSICIANS network resources are considered AFFILIATED PHYSICIANS property.

5.2. Users shall have no expectation of privacy in email and internet use.

5.3. AFFILIATED PHYSICIANS may monitor messages and internet use without prior notice.

5.4. Users are responsible for reporting any suspected or confirmed violations of this policy to their department manager or either the AFFILIATED PHYSICIANS Information Security Office or the AFFILIATED PHYSICIANSHS Office of Information Security.

5.5. Users shall not misuse their Internet privileges, i.e., spending excessive time on the Internet for non-work related business or accessing inappropriate sites.

5.6. Users shall not misuse their email privileges, i.e., sending and forwarding non-business related mass emails.

5.7 Users shall delete chain and junk email messages without forwarding or replying to them. Electronic chain letters and other forms of non-business related mass mailings are prohibited.

5.8. Personnel shall not use AFFILIATED PHYSICIANS resources to view, record, or transmit materials which violate AFFILIATED PHYSICIANS policies. Inappropriate messages, pictures, and/or other visual images/materials include, but are not limited to:

5.8.1. **Fraudulent messages** - Messages sent under an anonymous or assumed name with the intent to obscure the origin of the message.

5.8.2. **Harassment messages** - Messages that harass an individual or group for any reason, including race, sex, religious beliefs, national origin, physical attributes, or sexual preference.

5.8.3. **Obscene messages** - Messages that contain obscene or inflammatory remarks.

5.8.4. **Pornographic materials** -This includes, but is not limited to pictures, audio/video files, literature, or newsgroups.

5.9. Users shall not engage in spamming activities. Electronic chain letters and other forms of non-business-related mass mailings are prohibited.

5.10. Users shall not photograph, post, or transmit patient images or information, electronically or otherwise, unless doing so is in accordance with an approved use or disclosure, and approved methods for doing so are utilized.

5.11. Users shall not share sensitive, restricted, or protected health information (PHI) to any cloud provider that has not been approved by the Information Security Office (including but not limited to Google Apps, DropBox.com, GoogleDocs, iCloud, etc.).

5.12. Users shall not send or forward email containing sensitive, restricted, or protected health information (PHI) **to public email systems** (including but not limited to Hotmail.com, gmail.com).

5.13. Users shall not forward sensitive information, PHI, or other AFFILIATED PHYSICIANS business information to non-business-related email accounts, including but not limited to Gmail, Yahoo, iCloud,etc.

5.14. Personal email accounts shall not be used for official AFFILIATED PHYSICIANS business.

5.15 AFFILIATED PHYSICIANS reserves the right to block access to non-business-related material.

5.16 Email transmission of PHI, if necessary, shall be conducted with the highest level of security applied and only in situations where the email is necessary for the treatment of the patient, payment, and health care operations. For users of the Affiliated Physicians email system only: To send email transmissions over the Internet (outside the AFFILIATED networks), PHI and other sensitive information shall be encrypted. Email shall not be transmitted over the Internet from any other email system unless/until an encryption method is approved for that email system.

5.17. Users shall comply with all laws related to copyright, intellectual, and personal property.

5.18. Users shall check their email regularly and delete unneeded email.

5.19. Users shall not knowingly download non-work-related executable files from the Internet.

5.20. Users shall not establish peer-to-peer connections to external parties.

5.21. Users shall not knowingly enable anyone to gain unauthorized access or control of any device, application, or system to the data networks

5.22. Users shall report suspicious emails using the Report Phishing button or forwarded to helpdesk@innercircle.com.

5.23. For the AFFILIATED PHYSICIANS network, the use of any software or service that hides the identity of the user or the location of the user while using the Internet is prohibited (including but not liited to proxy bypass, anonymization networks such as Tor, and VPN connections).

5.24. Individuals may be granted access to the email account of their former employee or vendor with Human Resources approval. This may require written approval from requestor's supervisor.

5.24.1. The account shall be used only for the retrieval of existing email and shall not be user to impersonate the former personnel or send email communications on their behalf.

5.25. Users shall not utilize their AFFILIATED PHYSICIANS passwords on any non-corporate systems (i.e., banking, personal email, etc.).

5.26. Users shall not circumvent AFFILIATED PHYSICIANS technical security controls.

5.27. Users shall not transfer restricted or sensitive information to an unencrypted or unapproved device.

5.28. Users shall log off application, workstations, laptops, and devices after use.

5.29. Users shall not store restricted or sensitive information on non-AFFILIATED PHYSICIANS equipment such as personally-owned devices unless properly authorized to do so.

5.30. Users shall not provide personal or official AFFILIATED information solicited by unknown individuals or suspected phishing email or websites.

5.31. Users shall follow the same security policies at any alternate workplaces as those required on the AFFILIATED PHYSICIANS networks.

5.32. **CONTACTS:** For questions regarding the requirements, implementation, and enforcement of this standard, contact one of the following:

5.32.1. AFFILIATED PHYSICIANS Direct Manager

5.32.2. AFFILIATED PHYSICIANS HIPAA Security Office

5.32.3. AFFILIATED PHYSICIANS IT Data Security Office

6. ENFORCEMENT: Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or assignment, depending on the severity of the infraction. In addition, AFFILIATED PHYSICIANS may report the matter to civil and criminal authorities as may be required by law.