Elizaveta Vos

Week 2 Homework

**Acceptable Use Policy - Access EHR Software From Personal Device.**

**SCOPE**

This policy outlines the specific requirements for accessing Electronic Health Record (EHR) software from personal devices within the Hospital Authority. The use of computing and network resources in this context is crucial for supporting patient care activities within the hospital. Access to EHR software from personal devices is a privilege extended to authorized individuals within the Hospital Authority, and it is imperative that users adhere to responsible, ethical, and legally compliant practices.

**PURPOSE**

This policy applies to all employees, contractors, vendors, and any other individuals who access Electronic Health Record (EHR) software from personal devices within the large hospital system. The purpose of this policy is to ensure the secure and appropriate access of EHR software from personal devices while maintaining the confidentiality, integrity, and availability of sensitive patient information.

Computing resources encompass all hardware, software, data, and associated assets owned or managed by the Hospital Authority, as well as user accounts assigned by the institution. This policy extends to both University-owned equipment and personally owned devices connected to the Hospital Authority network, irrespective of physical location or connection method.

The policy's applicability spans across various administrative divisions and departments within the Hospital Authority. It is designed to ensure consistent adherence to security protocols and best practices, regardless of the technological environment or ownership status of the devices utilized.

**REQUIREMENTS**

In making acceptable use of resources, individuals covered by this policy must:

1. Authorized Use: Utilize resources solely for purposes authorized by the Hospital Authority, specifically for accessing and managing electronic health records.
2. Protection of Credentials: Safeguard User IDs, digital signatures, and other authentication mechanisms from unauthorized use. Users are responsible for all activities conducted under their credentials.
3. Access Control: Access only information for which authorization has been granted or that is publicly available.
4. Data Protection: Adhere to data security policies and relevant laws when handling electronic and hardcopy data classified as High-Risk or Moderate-Risk (confidential).
5. Software Compliance: Use only legally obtained versions of software in accordance with vendor license agreements.
6. Resource Consideration: Be considerate in resource usage, refraining from actions that monopolize resources or degrade services for others.
7. Limited Personal Use: Restrict personal use of EHR software to minimal and occasional activities consistent with applicable laws and Hospital Authority policy.
8. Content Relevance: Ensure that communications and materials shared within the EHR system are relevant to Hospital Authority matters.
9. Confidential Data Handling: Store confidential data in approved secure locations and transmit it only through authorized secure mechanisms.
10. BYOD Compliance: Use Bring Your Own Device (BYOD) only through approved methods designated by the Hospital Authority.
11. Security Incident Reporting: Promptly report any identified or suspected security incidents to the appropriate authorities.

In making acceptable use of resources, individuals covered by this policy must not:

1. Unauthorized Access: Attempting to access or use another individual's system, files, or data without proper authorization.
2. Password Sharing: Disclosing passwords or authentication means to any unauthorized individuals.
3. Security Measures Circumvention: Trying to bypass or undermine system or network security measures.
4. Malicious Activities: Engaging in activities intended to harm systems or compromise information integrity, such as creating or spreading malware.
5. Copyright Infringement: Making or using illegal copies of copyrighted software or transmitting such copies over hospital networks.
6. Misuse of Communication Tools: Using email, social networking platforms, or messaging services for unlawful purposes or to harass others.
7. Commercial Use: Utilizing hospital systems or networks for commercial purposes without authorization.
8. Unauthorized Representation: Making unauthorized use of Hospital Authority trademarks or logos or falsely claiming to represent the organization.
9. Violation of Laws and Policies: Breaching any applicable laws, regulations, or Hospital Authority policies governing IT resource usage.
10. Unsolicited Communications: Sending commercial or personal advertisements or solicitations unrelated to hospital business.
11. Insecure Transmission of Data: Sending or receiving confidential information over the internet without adequate security measures.
12. Unauthorized Data Modification: Modifying hospital information resources or technology without proper authorization.
13. Insecure Data Storage: Storing confidential data on local drives, external media, or unauthorized locations.

**RESPONSIBILITY**

* The hospital system's IT security team will conduct regular monitoring and auditing of access to EHR software from personal devices to ensure compliance with this policy.
* Access reviews will be conducted periodically to review access logs, identify any unauthorized activities, and ensure that access privileges are appropriate and up-to-date.
* Any anomalies or security incidents will be promptly investigated and addressed in accordance with the hospital system's incident response procedures.
* Failure to comply with this policy may result in disciplinary action, including the restriction or revocation of network privileges, in accordance with Hospital Authority policies and procedures.
* The hospital system's IT department is responsible for updating and enforcing this policy. They are tasked with regularly reviewing and updating the policy to reflect changes in technology, regulations, and security best practices. Additionally, they are responsible for enforcing compliance with this policy and imposing disciplinary actions for violations.