Heart-Healthy Insurance Information Security Policy

You are the manager of the information security analyst team for a large health insurance company. Your supervisor has asked you to review and provide recommendations for changes to the company's information security policy. The intent of this review is to ensure that the policy complies with current regulatory requirements, obtains the benefits of industry specific standards, utilizes a recognized framework, is relevant for your company, and meets the requirements of all relevant regulations and standards. The review's outcome should be to recommend modifications to the policy to ensure alignment with relevant regulatory requirements.

The policy is a large document that discusses confidentiality, integrity, and availability across the spectrum of the electronic information systems that your company utilizes. Among the services that your company provides are patient-history evaluations for chronic illness indicators, insurance rate underwriting, paying claims to healthcare providers, accepting premium payments from employers, and accepting copayments from claimants.

In addition to regulatory requirements, the U.S. Department of Health and Human Services (HHS) has set some national standards for identification of employers, providers, transactions, procedure codes, and place of service codes.

The company you work for holds information that is protected by regulatory requirements. This information includes individual privacy information, personal health information, financial information, and credit information. Information about employees and patients, also known as demographics, contain personally identifiable information, which is covered under the U.S. Federal Privacy Laws. Health information that is personally identifiable, also known as PHI, is required to be protected under HIPAA and HITECH. Because the company is an insurance company the government classifies the company as a financial institution, it is required to comply with the GLBA. Also, the company takes credit cards to pay for premiums and deductibles and consequently must be PCI-DSS compliant.

Of greatest concern to your supervisor are the sections of the policy that stipulate how a new user is provided access to information systems and the password requirements for those systems.

New Users

The current new user section of the policy states:

> *"New users are assigned access based on the content of an access request. The submitter must sign the request and indicate which systems the new user will need access to and what level of access will be needed. A manager's approval is required to grant administrator level access."*

Password Requirements

The current password requirements section of the policy states:

> *"Passwords must be at least eight characters long and contain a combination of upper- and lowercase letters. Shared passwords are not permitted on any system that contains patient information. When resetting a password, users cannot reuse any of the previous six passwords that were used. Users entering an incorrect password more than three times will be locked out for at least 15 minutes before the password can be reset."*