Sensitive Health Data and Privacy

Author: Jason Ludwig, Dalton George

Summary: *A tech company contracts Luminia, a healthcare information firm, to design an employee wellness program. The President of Luminia recommends that the company implement a secure messaging platform to protect employee's private health information (PHI). The company's vice president, however, thinks that the platform is too expensive and that the extra protection is unnecessary.*

Three years ago, Dave started his own healthcare information firm, Luminia. The firm has recently received a contract from Samson Solutions, a large tech company that wants to curb its healthcare costs by starting a workplace wellness program. Employees are given the option of participating in the program, and those who do participate will receive a discount on their insurance premiums in exchange for granting Luminia access to their private health information (PHI). Luminia will use this data to develop an app that will predict employees' health needs and recommend treatment. For example, an employee determined to be at risk for diabetes might get a personalized message through the app suggesting that they visit a doctor or join a weight-loss program.

Every month, Dave meets with Lisa, Samson's Senior Vice President in charge of human resources, to review Luminia's progress in designing the application. In one meeting, they begin discussing the security protections that will be built into the application. They agree that employees' PHI will be stored on a cloud server that meets Health Insurance Portability and Accountability Act (HIPAA) standards for health data encryption. Since many of the employees will be accessing messages from the application on their mobile devices, such as laptops or smart phones, Dave also recommends that they implement a highly-reviewed secure messaging platform. The platform will ensure that PHI remains encrypted while it is in transit between the cloud server and mobile devices, and once it is stored on user's laptops and smartphones. This way, if one of Samson's employees has their phone or laptop stolen, the thief will be unable to access employees' PHI.

Lisa, however, thinks that the secure messaging platform is too expensive. Designing the application has already cost the company more than was anticipated and she is reluctant to make

any additional expenditures. “Plus,” she states, “the cloud server already meets HIPAA standards for data encryption, so this would just be unnecessary.”

Dave tells her that he thinks that not purchasing the secure messaging platform is a mistake. It will leave employees’ sensitive health data extremely vulnerable. “Lost and stolen devices have been major causes for data breaches and PHI exposure,” he explains. “Without further encryptions, someone could potentially gain access to information containing employees’ names, Social Security numbers, addresses, and medical conditions.” Lisa refuses to listen to his argument, and will not authorize the extra protection.

Questions

1. What professional and/or ethical responsibilities does Dave have towards the employees whose health data he will handling?
2. If the cloud server already meets the HIPAA requirements for data protection, is the secure messaging platform unnecessary?
3. Why might a software designer go above and beyond HIPAA requirements to protect private health information (PHI)?

Resources

Appleby, Julie. “Advocates Urge Protection of Employee Health Data.” *CNN*. http://www.cnn.com/2015/09/29/health/protecting-employee-health-data-exclusive/index.html.

“HIPAA Encryption Requirements.” *HIPAA Journal*. http://www.hipaajournal.com/hipaa-encryption-requirements/.

“Patients Warned of PHI Exposure After Premier Healthcare Laptop Theft.” *HIPAA Journal*. http://www.hipaajournal.com/patients-warned-of-phi-exposure-after-premier-healthcare-laptop-theft-3347/

Jason Ludwig, MS, and Dalton George, MS, are graduates of the Drexel University Center for Science, Technology and Society. June 2017.