CSEC 751.01 – HIPAA In Class Exercise - Fall 2024

PLEASE DOWNLOAD and use your own copy. Once you have completed this document – upload it to your folder in the Google drive provided by Vishal.

	Line Number	Words or statement (copy and paste it here)	Explanation as to why it proves lack of compliance with HIPAA and the safeguard (or code language) which addresses the requirement
1	39	Plain Text	HIPAA requires PHI to be stored in an encrypted manner – Technical Safeguard of the Security Rule – Access Control Standard - Addressable
2	71-74	Predefined PHI definitions. Fields categorized as PHI are encrypted at rest – Based on HIPAA definitions these include All medical information without exception. It also includes other critical information considered PHI, which includes all credit card payment information received by insurance companies.	The Security Rule protects a subset of information covered by the Privacy Rule, all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. The Security Rule allows EPHI to be sent over an electronic open network as long as it is adequately protected.
			These individual notifications must be provided without unreasonable delay and in no case later

			than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable). Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices
3	**128-129**	**Automatic breach reporting to patients can be set up with a minimum of 60 days and a maximum of 120 days mailing window from the date the system is coded as breached. This feature provides the peace of mind that HIPAA reporting requirements are timely addressed**	

			electronically. **60 is the limit and reports are sent by what method is not specified**
4	**119-121**	**…for an additional nominal cost and with no further contractual needs, customer records can be accessed 24X7 by our staff and emailed to you on an as needed basis. Records can be saved and shared with you using different formats (word, PDF to txt files.)**	**The Security Rule protects a subset of information covered by the Privacy Rule, all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. The Security Rule allows EPHI to be sent over an electronic open network as long as it is adequately protected.** **Internet may not be secure**
5	**123-124**	**Grey Hippo by default, automatically and simultaneously sends patients' information to their main physicians, family members, insurance companies and government agencies.**	**Covered entities must provide only the minimum necessary access to EPHI that is required for a workforce member to do his or her job.** **This does not specify what information or if all the information is being sent to other entities**

6	**99-101**	**Security of systems is paramount for HIPAASecureIsUs, Inc. That is why access to Grey Hippo requires the use of a two-factor authentication: unique usernames in combination with hard to guess passwords create dual defense barrier to mitigate inappropriate access.**	**Covered entities must train all users and establish guidelines for creating passwords and changing them during periodic change cycles.** **Change of passwords is not mentioned**
7	**113-116**	**Data Storage and reporting: Customer records are stored in one singular cloud-based database – Users who only need to view reports (who have a username with an R at the end of it) are expected to only view records within Grey Hippo. Reporting users can tailor reports by simply dropping and dragging fields into over 20 reporting templates.**	**The Data Backup Plan implementation specification requires covered entities to: "Establish and implement procedures to create and maintain retrievable exact copies of electronically protected health information.** **No backup is mentioned. A singular cloud-based database is not sufficient.**
8	**84-85**	**Our application covers: The Privacy Rule Scheme, The Security Rule Scheme and the Management Reporting Rule Scheme**	**HIPAA has 3 main regulatory schemes: Privacu rule, security rule, and breach notification notice**

9	**99-105**	**Security of systems is paramount for HIPAASecureIsUs, Inc. That is why access to Grey Hippo requires the use of a two-factor authentication: unique usernames in combination with hard to guess passwords create dual defense barrier to mitigate inappropriate access. Role-based protection is a requirement of HIPAA and it is provided by assigning usernames that reflect the type of work the perform in the system. For example: Patient Managers have the letters PM at the end of their usernames. This allows for user roles to be easily identified when reviewing logs. Log reviewers can determine if access or modification of fields was authorized based on the person's role.**	**it seems like all users are allowed to access the application. User roles are not clearly defined. Administrative safeguards require that, applications: Implement policies and procedures for authorizing access to electronic protected health information that is consistent with the applicable requirements of subpart E of this part [the Privacy Rule]**

10	**107-111**	**Procedural mechanisms to record and examine access and other activity in Grey Hippo provide great security controls. The system records every key stroke, including username and time/date stamp of each stroke. This information is saved in a .txt file in our public cloud environment. By providing customers with a unique, tailor branded website for access, a logical separation between our customers is established, providing a superior security control**	**Potential Exposure of PHI: Recording every keystroke, including usernames, timestamps, and potentially sensitive data, could expose PHI or other sensitive information. Under HIPAA, access to PHI must be limited, and any recording or tracking of data must be done securely to prevent unauthorized access or disclosure.** **HIPAA's Security Rule requires implementing administrative, physical, and technical safeguards to protect electronic PHI (ePHI). Recording every keystroke and storing that data in a public cloud could expose sensitive information, making it more vulnerable to unauthorized access or breaches.**

11	**136-137**	**Create concise record reports that can be used to increase the profitability of your organization by leasing patient information to pharmaceutical research and marketing**	**Unauthorized Use of PHI: Leasing or selling patient information to pharmaceutical companies for marketing or research purposes without explicit authorization from the patients is a direct violation of HIPAA. PHI cannot be shared for marketing purposes without the patient's consent. Even if the data is de-identified, strict rules govern the sharing of such data.** **Marketing Violations: HIPAA prohibits the use of PHI for marketing purposes unless the patient has provided explicit written permission. Leasing patient data for profitability or marketing purposes is considered a marketing activity, which would require patient authorization.**

12	**138**	**Link records with Ivy League universities for advancements in medical research**	**Research Rules under HIPAA: Sharing PHI with universities for medical research can be allowed, but only under specific conditions, such as obtaining patient consent or a waiver of authorization from an Institutional Review Board (IRB). If this data is shared without meeting these requirements, it would violate HIPAA.** **If the data is de-identified (meaning all personal identifiers have been removed), it can be shared more freely. However, if identifiable patient data is shared without following the appropriate authorization or waiver process, this would be a breach of HIPAA.**

13	**124-126**	**As an increased security control, explicit approvals by the CISO are required before sending information to business partners or other external parties (health clubs, online diet programs, etc.)**	**If the information being sent includes PHI, sharing it with external parties such as health clubs or online diet programs may violate HIPAA unless there are specific safeguards and agreements in place.** **Under HIPAA, PHI can only be shared with external parties if they are Business Associates who have signed a Business Associate Agreement (BAA). The BAA ensures that the external party will safeguard PHI in compliance with HIPAA's rules. Health clubs and diet programs would likely not qualify as Business Associates unless they are performing specific healthcare operations on behalf of a covered entity.**
			Family Members: Under HIPAA, healthcare providers may only share PHI with family members if the patient has given explicit authorization or if the disclosure is directly related to the patient's care

			and the patient has not objected. Automatically sending patient information to family members without patient consent would be a clear violation of HIPAA's Privacy Rule.
14	**123-124**	**Grey Hippo by default, automatically and simultaneously sends patients' information to their main physicians, family members, insurance companies and government agencies.**	**Information is being shared with government agencies, insurance companies, etc…:** **Automatically sending PHI to multiple entities without considering the specific needs and permissions of each party is problematic.** **HIPAA requires that each disclosure of PHI be justified and minimized to only what is necessary. Sending large amounts of PHI to parties who may not need all of it increases the risk of unnecessary exposure to sensitive patient information.**

15	**128-129**	**Automatic breach reporting to patients can be set up with a minimum of 60 days and a maximum of 120 days mailing window from the date the system is coded as breached. This feature provides the peace of mind that HIPAA reporting requirements are timely addressed**	**Method of reporting, patient consent for email, is not mentioned**

Feel free to add more lines to this, if you want to share further findings.