**PlaceboPharama: (All quoted directly from management brief)**Currently investing in advanced cybersecurity measures to safeguard data and reduce risk of potential breaches.

Currently strengthening its third-party risk management in order to: secure its supply chain, data management, protect its proprietary research, and maintain high standards of excellence which make it the leader in the pharmaceutical industry.

**HIPAA:**

**What:** Health Insurance Portability and Accountability Act

**Why:** U.S law enacted in 1996 to protect sensitive patient health information **Why would companies want to implement this? Are there fines? What is the business impact on implementing or not implementing this?**

**Info:**

* Creates national standards for handling protected health information (PHI)
* Two key rules
  + Privacy rule: Regulates how PHI is used and disclosed
  + Security rule: Sets standards for protecting electronic PHI (ePHI)

**Specifics: (Stuff that we already do to comply with hipaa, pick and choose from this list to write in reports)**

Administrative Safeguards:

* Risk Analysis (§164.308(a)(1)(ii)(A)): Perform a periodic risk analysis to identify vulnerabilities.
* Risk Management (§164.308(a)(1)(ii)(B)): Implement measures to mitigate identified risks.
* Workforce Training (§164.308(a)(5)): Train all employees on HIPAA policies and PHI protection.

Physical Safeguards:

* Workstation Use (§164.310(b)): Define policies on workstation security and usage.

Technical Safeguards:

* Access Control (§164.312(a)): Implement unique user IDs, automatic logoff, and encryption for ePHI.
* Audit Controls (§164.312(b)): Monitor and log system activity.
* Transmission Security (§164.312(e)): Encrypt ePHI during transmission over networks.

**HITECH:**

**What:** Health Information Technology for Economic and Clinical Health Act

**Why:** U.S law enacted in 2009 to promote the best practices in using electronic health records (EHRs) **Why would companies want to implement this? Are there fines? What is the business impact on implementing or not implementing this?**

**Info:**

* Builds upon and strengthens HIPAA
* Gives stricter penalties for not following HIPAA
* Expands scope of HIPAA
* Introduces “Breach Notification Rules” requiring entities to notify individuals and government of data breaches involving PHI