# Compliance and Regulations

IT security has a variety of laws and regulations that one must be aware and adhere. Pick three items from the attached list. Give a brief history of the regulation or law and how it pertains to IT security. For the final part of this assignment, put yourself in the role of an IT Security Officer for a local Ohio hospital. List the laws and regulations that would pertain to an online breach of 10,000 patient records with identifiable data such as SSN and payment history.

List:

* HIPAA
* FERPA
* SOX
* PCI
* FISMA
* GLBA
* CIPA
* State Laws (pick 1 state of your choice)

# Course Outcomes

Summarize compliance laws relevant to IT within a given industry.

HIPAA is the Health Insurance Portability and Accountability Act which was created to protect patient information from being disclosed without the patient's consent. It came around in 1996 and is a federal law put in place by the Department of Health and Human Services to protect the privacy of patients. It pertains greatly to IT security as most patient data is now saved in online databases instead of paper meaning that IT oversees protecting the digital records.

SOX is the Sarbanes-Oxley ACT which was passed in 2002 to protect people from accounting errors and fraud. It makes sure that when companies are releasing information that it is accurate. IT security is affected by this act as it looks at the records that are being kept and making sure there are no problems.

GLBA is the Gramm-Leach-Bliley Act which came about in 1999 as a law. This act focuses on financial companies such as banks or loan providers. IT security is affected by this as it means that the information sharing practices must have appropriate safeguards especially as it handles the finances.

A breach of 10,000 patients with their data including social security number and payment history would affect the following laws:

HIPAA- patients did not consent.

SOX-a lot of people will have their information taken and possibly used in fraudulent acts.

PCI- payment history was not secure.

FISMA- might not have followed the security guidelines so they will check.

GLBA- payment history leak affects banks and loan providers.

Some breaches are obvious such as the HIPAA violation while some need to be checked such as FISMA.

Centers for Disease Control and Prevention. (2022, June 27). *Health Insurance Portability and accountability act of 1996 (HIPAA)*. Centers for Disease Control and Prevention. Retrieved September 18, 2022, from https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

*Fisher Phillips how to analyze a HIPAA BREACH*. Fisher Phillips. (n.d.). Retrieved September 18, 2022, from https://www.fisherphillips.com/news-insights/how-to-analyze-a-hipaa-breach-1.html

Horan, M. (2019, September 25). *Regulatory compliance: The differences between HIPAA, Sox, and glba*. FTP Today. Retrieved September 18, 2022, from https://www.ftptoday.com/blog/regulatory-compliance-with-hipaa-sox-and-glba

*Privacy act issues under Gramm-Leach-Bliley*. FDIC. (n.d.). Retrieved September 18, 2022, from https://www.fdic.gov/consumers/consumer/alerts/glba.html

US Department of Education (ED). (2021, August 25). *Family educational rights and privacy act (FERPA)*. Home. Retrieved September 18, 2022, from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html