**Sprint Four: Legal Compliance**

**Group Members Responsible:**

**What does it mean the differences between a cybersecurity secure program being legal?**

**Legal**: When a cybersecurity secure program is legal, it means that it adheres to the laws and regulations applicable to cybersecurity and data protection. ***It ensures that the program meets the minimum legal requirements set by governing bodies.*** Compliance with legal requirements helps avoid legal consequences and penalties.

**Compliance**: Compliance refers to the act of adhering to all applicable legal requirements, regulations, and standards. ***A cybersecurity secure program is considered "in compliance" when it fulfills all the necessary obligations, both legal and regulatory.*** Compliance demonstrates that the program meets the required standards and best practices.

**Legal: Your research and writing should answer the following questions (with APA Cited References):**

* **What federal laws does a cybersecurity secure program for a non-profit have to adhere to? (What are the federal legal requirements a cybersecurity security program must comply with?)**
* **What New York State laws does a cybersecurity secure program for a non-profit have to adhere to? (What are the federal legal requirements a cybersecurity security program must comply with?)**
* **Why does the cybersecurity program have to adhere to this specific federal or state law? (For example, it’s because they take online payments.)**
* **What does the cybersecurity secure program have to contain or offer to satisfy or adhere to (federal or state law being discussed)?**
* **Are there any California, Georgia or New Jersey state laws applicable to a cybersecurity secure program for an NPO (as TKH operates in CA, GA and NJ)?**
* **What are the penalties for violating federal law to the non-profit in this instance?**
* **What are the penalties for violating state law to the non-profit organization?**
* **Relate it back to regulatory compliance:** 
  + **What cybersecurity frameworks are being followed when a cybersecurity secure program is following [insert law here]?**
  + **What regulations are being followed when a cybersecurity secure program is following [insert law here]?**

**Preliminary Research**

**What federal laws address the security of data assets and confidential digital information in a non-profit organization?**

Several federal laws address the security of data assets and confidential digital information in non-profit organizations. These laws are designed to protect personal information, ensure data privacy, and establish security standards. Here are some key federal laws:

1. The Health Insurance Portability and Accountability Act (HIPAA): HIPAA applies to non-profit organizations that handle protected health information (PHI). It sets privacy and security standards for maintaining the confidentiality, integrity, and availability of PHI. Non-profit organizations that provide healthcare services or handle health information must comply with HIPAA regulations to protect patient data.
2. The Gramm-Leach-Bliley Act (GLBA): The GLBA applies to non-profit organizations that engage in financial activities, such as handling financial transactions or providing financial services. It requires organizations to implement safeguards to protect the security and confidentiality of non-public personal information (NPI) of their customers.
3. The Family Educational Rights and Privacy Act (FERPA): FERPA applies to educational institutions, including non-profit organizations, that receive federal funding. It protects the privacy of student education records and restricts the disclosure of personally identifiable information (PII) from student records.
4. The Children's Online Privacy Protection Act (COPPA): COPPA regulates the collection and use of personal information of children under the age of 13 by websites and online services. Non-profit organizations that operate websites or online services directed towards children must comply with COPPA requirements to protect children's privacy.

References

U.S. Department of Health & Human Services. (n.d.). Health Information Privacy. Retrieved from<https://www.hhs.gov/hipaa/index.html>

Federal Trade Commission. (n.d.). Financial Privacy, Identity Theft, and Fraud. Retrieved from<https://www.ftc.gov/privacy-and-security/financial-privacy>

U.S. Department of Education. (n.d.). FERPA for Parents and Eligible Students. Retrieved from<https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Federal Trade Commission. (n.d.). Protecting Kids' Privacy Online. Retrieved from<https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy>

**What New York State state laws are concerned with the security of data and digital assets in a non-profit organization?**

In New York State, data assets and digital confidential information in non-profit organizations are governed by various laws and regulations. Here are some key laws that may be relevant:

1. New York General Business Law (GBL) § 899-aa: This law pertains to data breach notification requirements. It requires businesses, including non-profit organizations, to notify affected individuals and the New York State Attorney General in the event of a security breach involving private information.
2. New York Education Law § 2-d: This law specifically applies to educational agencies, including certain non-profit organizations involved in education. It establishes requirements for data privacy and security, including the protection of personally identifiable information (PII) and the adoption of data security and privacy policies.
3. New York Nonprofit Revitalization Act: Although not directly focused on data assets and digital confidential information, this act introduced several provisions relating to the governance and operations of non-profit organizations in New York State. It includes requirements for proper oversight and management of non-profit resources, which can indirectly impact the handling of digital information.
4. New York General Business Law (GBL) Article 39-F: This law establishes requirements for the protection of personal information held by businesses, including non-profit organizations. It mandates reasonable security measures to safeguard personal information and provides guidelines for data breach notification in the event of a security breach.

References:

New York State Senate. (2019). Laws of New York. Retrieved from<https://www.nysenate.gov/legislation/laws/GBS/899-AA>

New York State Education Department. (n.d.). Education Law Article 2-D. Retrieved from<http://www.counsel.nysed.gov/portal/sites/default/files/reports-and-materials/SAM_Education_Law_Article_2-D.pdf>

New York State Senate. (2013). Laws of New York. Retrieved from<https://www.nysenate.gov/legislation/laws/NPRA/7>

New York State Senate. (n.d.). General Business Law Article 39-F. Retrieved from<https://www.nysenate.gov/legislation/laws/GBS/39-F>