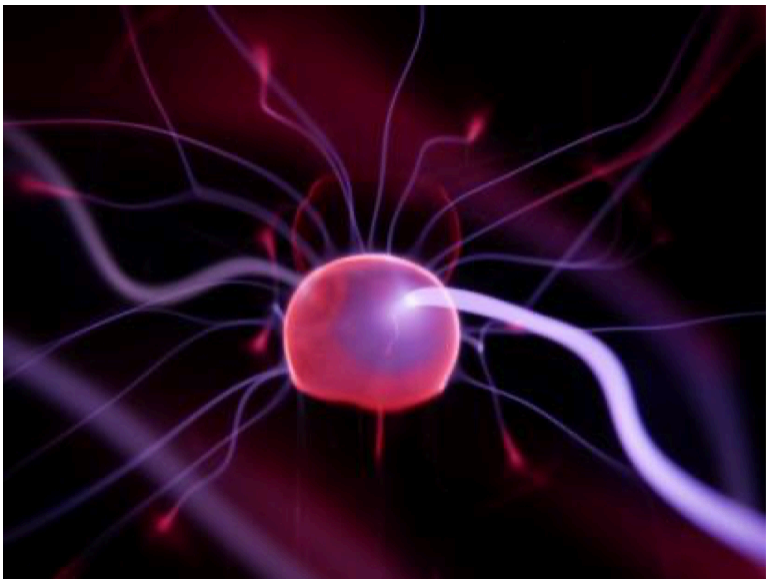
Surge Consulting



Expansion Proposal
Prepared for Binghamton Health Clinic
Created by Anthony Frick
07.20.2025

Topic	Findings and Recommendations
Regulatory Bodies	Regulation and standards can help organizations mitigate risks that come with the collection and usage of personal data and helps with users from having their personal data exposed. ● "To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security." OCR (2024) ● According to the OCR (2021) the office for civil rights is responsible for enforcing the privacy and security rules which began on 2003 for most HIPPA covered entities. The OCR has taken corrective action which has resulted in systemic change which in return has improved privacy protection of health information for all individuals served. ● For scenario A it would be more than likely that this request would be denied unless said family members were authorized for such information. If not authorized then this would be a breach of HIPPA and create grounds for legal action. For scenario B this would be allowed under HIPPA since this medical information is necessary for proper treatment of a patient and continuing care.

Topic	Findings and Recommendations
Impact of Data Regulation	● Ratcheting up or down on HIPPA and PHI would impact organizational policies without a doubt. Starting with the scenario of HIPPA becoming even more restrictive we could see changes like unique user identification for detailed audit logs and multi factor authorization forms. ● If we were to become more relaxed on regulation than scenario A regarding the patients family member requesting information would be no problem at all. Which does beg the question even though federal laws have become more relaxed does that mean your own institutional policies need to be as well? My opinion is no, especially when it comes to PHI. Eroding trust between patients and healthcare professionals is what you would be setting yourself up for in doing so. ● Lastly scenario B would be unaffected by this since either way the medical facility would still need a patients PHI in order for proper treatment of a patient and continuing care.
Regulating Data Usage	● The pros and cons of handling sensitive data versus non sensitive data. Increased trust and reputation along with a competitive edge would be the two pros for proper handling since your credibility is boosted and in return comes long term loyalty among clients. Compliance burden and security risks would be the cons for handling such information expect increased costs for implementing additional security based hardware like sonic walls, servers, storage, software and possibly a third party second security check to further protect against possible data leaks. ● If the client is unsure on how to properly handle sensitive data then they should not be in the position to do so until they've been educated on doing so and can make a professional judgement when its time to do so no exceptions. ● Proper training for employees is a must when it comes to handling sensitive and non sensitive data. Typically a SOP (standard operations protocol) and yearly training would be sufficient to get staff up to speed and in compliance.

Topic	Findings and Recommendations
Data Professional Roles	● Roles for individuals that would be responsible for enforcing these regulations across an organization would be data security officers and possibly network admins. ● With data security officers being responsible for audit logs of employee interaction and use of PHI and if those individuals are appropriately accessing information that pertains to the role in which they are responsible for in relation to patient care. ● Network admins would be responsible for surveying the network and having proper systems in place for things like a malware, trojan horse, social engineering attack. Lastly admins should be checking for any data being exported from any computer in the organization as this too could be someone stealing or leaking PHI. ● Regulatory bodies in charge of enforcing regulations for the client would be the OCR as mentioned before.

References

(OCR), O. for C. R. (2021, June 28). *HIPAA compliance and Enforcement*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

(OCR), O. for C. R. (2024, July 19). *HIPAA for professionals*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/index.html