Abstract:

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 effectively establishes a standard of due care for healthcare information security. One of the challenges of implementing policies, procedures, and practices consistent with HIPAA requirements in the Department of Defense Military Health System is the need for a method that can tailor the requirements to a variety of organizational contexts. This paper will describe a self- directed information security risk evaluation that will enable military healthcare providers to assess their risks and to develop mitigation strategies consistent with HIPAA guidelines.

The Health Insurance Portability and Accountability Act (**HIPAA**) Security Rule requires that covered entities and its business associates conduct a **risk assessment** of their healthcare organization. ... A **risk assessment** also helps reveal areas where your organization's protected health information (PHI) could be at **risk**.

he HIPAA Security Rule was enacted to protect personal health information (PHI) by putting national standards and safeguards in place. This Security Rule included a safeguard for “Risk Analysis.”

What Does HIPAA Compliance Entail?

HIPAA (Health Insurance Portability and Accountability Act of 1996) is US legislation that provides data privacy and security provisions for safeguarding medical information.

HIPAA applies to any entity that takes healthcare insurance and any entity that provides healthcare services. The main purpose of HIPAA is to standardize the tracking and security of electronic healthcare transactions. HIPAA compliance requires organizations to implement safeguards that protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).

Organizations who wish to achieve HIPAA compliance will benefit from HIPAA compliance checklists and HIPAA compliance software, which enables healthcare providers to meet requirements while simultaneously increasing efficiency.

**What Are the Benefits of HIPAA Compliance Software?**

Healthcare recordkeeping is moving full speed ahead, and will soon be entirely paperless. Few hospitals and insurance offices still keep hard copies of patient files safely guarded behind lock and key. The shift to electronic health records (EHR) has brought many benefits: greater efficiency, wider access, and seamless communication between practitioners and provider networks.

However, by putting information (once only exposed to physical threats such as break-ins or fires) in digital format, we open an entirely new realm of threats that must be mitigated. Faulty hardware, insufficient authentication, inadequate backups, and unintentional disclosures are now pervasive threats across all healthcare and service providers.

HIPAA risk assessment software empowers healthcare organizations to ensure threats are managed proactively and effectively without letting incidents fall through the cracks. Logic Manager’s unique risk-based approach to HIPAA risk management enables your business to monitor and report on the effectiveness of your HIPAA compliance process, all while leveraging our pre-built HIPAA checklists and risk assessments.

**What Are the Benefits of HIPAA Compliance Software?**

Healthcare recordkeeping is moving full speed ahead, and will soon be entirely paperless. Few hospitals and insurance offices still keep hard copies of patient files safely guarded behind lock and key. The shift to electronic health records (EHR) has brought many benefits: greater efficiency, wider access, and seamless communication between practitioners and provider networks.

However, by putting information (once only exposed to physical threats such as break-ins or fires) in digital format, we open an entirely new realm of threats that must be mitigated. Faulty hardware, insufficient authentication, inadequate backups, and unintentional disclosures are now pervasive threats across all healthcare and service providers.

HIPAA risk assessment software empowers healthcare organizations to ensure threats are managed proactively and effectively without letting incidents fall through the cracks. LogicManager’s unique risk-based approach to HIPAA risk management enables your business to monitor and report on the effectiveness of your HIPAA compliance process, all while leveraging our pre-built HIPAA checklists and risk assessments.

What Is Integrated ERM?

Integrated ERM brings all risks from across the enterprise together to determine how they interrelate uncovering insights that have previously been hidden within individual silos. The often-cited benefits of adopting Integrated ERM within healthcare institutions include:

High-quality patient care: In addition to effectively highlighting patient safety issues that can then be resolved, Integrated ERM also enables healthcare organizations to more easily adopt increasingly popular patient-centered value-based care models.

Compliance: While Integrated ERM is not about managing risk solely to meet compliance requirements, compliance is often a benefit of taking risks out of silos, obtaining a comprehensive view of those risks, and uncovering a plan of action that goes well beyond compliance standards.

Resilience Because Integrated ERM accounts for both the upsides and downsides of risk, it can help organizations to better withstand hazards, as well as thrive in the wake of a changing marketplace when value-enhancing risks are taken, like adding a profitable new clinical business line, or merging with other providers

Proper Investment Integrated ERM hinges on well-founded data that can rank your risks and offer insight on where to invest. Whether you invest in risk mitigation or value-incented risk-taking, you can feel more confident about your spend.

Improved Processes Integrated ERM can eliminate redundancies that often transpire due to operating in silos. The resulting transparency and collaboration means less likelihood of creating additional problems in one area after solving for a problem in another area.