Oct 20th, 1:25 PM - 1:50 PM

Towards a Development of Predictive Models for Healthcare HIPAA Security Rule Violation Fines

Jim Furstenberg
Nova Southeastern University, jf1567@mynsu.nova.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Abstract
The Health Insurance Portability and Accountability Act's (HIPAA) Security Rule (SR) mandate provides a national standard for the protection of electronic protected health information (ePHI). The SR's standards provide healthcare covered entities (CEs') flexibility in how to meet the standards because the SR regulators realized that all health care organizations are not the same. However, the SR requires CEs' to implement reasonable and appropriate safeguards, as well as security controls that protect the confidentiality, integrity, and availability (CIA) of their ePHI data. However, compliance with the HIPAA SR mandates are confusing, complicated, and can be costly to CEs'. Flexibility in the SR's design and its facility-centric approach leave CEs' at a disadvantage; it appears that there is no clear SR compliance benchmark or standard to measure up against to ensure compliance, while the Office of Civil Rights (OCR) fine companies for non-compliance. This work-in-progress study examines the preponderance of failed HIPAA compliance audits, regarding SR regulations in healthcare CEs. SR non-compliance puts CEs at significant risk of monetary loss via sanctions, fines, and penalties from regulatory audits and data disclosure investigations (i.e. OCR). Furthermore, disclosures of deeply sensitive ePHI can result in any number of critical issues, including a patient's medical identity theft, financial fraud, and even problems that can negatively impact a patient's medical treatment decision-making, or the treatment itself. The primary goal of this work-in-progress study is to develop predictive models of CEs HIPAA SR violation fines, based on past OCR enforcement actions and weighted SR controls by current subject matter experts (SMEs); to empirically assess the compliance as well as security posture of ePHI data. Furthermore, this work in progress study will extend the Theory of Regulatory Compliance (TRC), into the healthcare knowledge domain by identifying those critical SR controls that are predictive in reducing non-compliance penalty exposure(s).

Keywords: HIPAA Security Rule, HIPAA compliance, critical security controls, healthcare cybersecurity, electronic protected health information

Location
KC 460

Disciplines
Information Security | Management Information Systems | Technology and Innovation

Towards a Development of Predictive Models for Healthcare HIPAA Security Rule Violation Fines

ABSTRACT

The Health Insurance Portability and Accountability Act's (HIPAA) Security Rule (SR) mandate provides a national standard for the protection of electronic protected health information (ePHI). The SR's standards provide healthcare covered entities (CEs') flexibility in how to meet the standards because the SR regulators realized that all health care organizations are not the same. However, the SR requires CEs' to implement reasonable and appropriate safeguards, as well as security controls that protect the confidentiality, integrity, and availability (CIA) of their ePHI data. However, compliance with the HIPAA SR mandates are confusing, complicated, and can be costly to CEs'. Flexibility in the SR's design and its facility-centric approach leave CEs' at a disadvantage; it appears that there is no clear SR compliance benchmark or standard to measure up against to ensure compliance, while the Office of Civil Rights (OCR) fine companies for non-compliance. This work-in-progress study examines the preponderance of failed HIPAA compliance audits, regarding SR regulations in healthcare CEs. SR non-compliance puts CEs at significant risk of monetary loss via sanctions, fines, and penalties from regulatory audits and data disclosure investigations (i.e. OCR). Furthermore, disclosures of deeply sensitive ePHI can result in any number of critical issues, including a patient's medical identity theft, financial fraud, and even problems that can negatively impact a patient's medical treatment decision-making, or the treatment itself. The primary goal of this work-in-progress study is to develop predictive models of CEs HIPAA SR violation fines, based on past OCR enforcement actions and weighted SR controls by current subject matter experts (SMEs); to empirically assess the compliance as well as security posture of ePHI data. Furthermore, this work in progress study will extend the Theory of Regulatory Compliance (TRC), into the healthcare knowledge domain by identifying those critical SR controls that are predictive in reducing non-compliance penalty exposure(s).

Keywords: HIPAA Security Rule, HIPAA compliance, critical security controls, healthcare cybersecurity, electronic protected health information