ABSTRACT

Healthcare organizations face significant data breach risks due to human error, despite technological advancements. Despite previous research, we still don't fully understand how individual, organizational, and technical factors affect healthcare security behavior. This study explores the role of individual, organizational, and technical factors in shaping information security compliance and protection behavior in healthcare institutions. Utilizing the Stimulus-Organism-Response model, the research investigates how external pressures, such as information security regulations and policies, alongside internal factors like security training and education, incident experience, and technical controls, influence employee behavior and awareness. Findings reveal that while technical measures are essential, human factors—especially security awareness—are pivotal in preventing breaches. This paper proposes a conceptual framework for compliance and protection behavior based on the stimulus-organism-response model.

Keywords: *information security compliance, healthcare cybersecurity, stimulus-organism-response model*