



*University of Utah*

UNDERGRADUATE RESEARCH JOURNAL

**PATIENT PRIVACY AND DATABASE SECURITY  
FOR EMERGING HEALTH INFORMATION TECHNOLOGY**

**Chloe Garner (Supervised by Rebecca Utz, PhD)**

**Department of Social and Behavioral Science**

The field of health information technology has exploded over the last decade. With new innovations and technologies evolving quickly, government regulations and policies in place to protect patient information have been created as a response to the changing field, instead of as a way to shape the booming health IT field. The policies currently in place to protect patient privacy and secure databases containing protected health information (PHI) are insufficient. As hacking incidents are on the rise, the need for new regulatory implementation is at an all-time high. However, a major issue currently exists in the field of health information technology: a lack of interoperability. Because electronic health records (EHRs) are housed by different vendors across the nation, there is not a system that allows for communication between the varying databases. Primary Children's Hospital, for example, uses a Cerner system while the University of Utah Hospital has implemented Epic to house their EHRs. Opening communication among the various vendors may increase interoperability and improve the patient experience but doing so would also create vulnerabilities in the system, which could result in adversaries stealing patient information. Implementing new privacy and big data laws, as well as creating a minimum standard for database security, are just some of the potential ways in which this field can be better protected and regulated. Ensuring that both the patient and physician perspectives on patient privacy and database security are assessed would allow for proposition and assessment of potential solutions to the issues that currently face this field.