NOTES AND COMMENTS

The Need for Privacy-Centric Role-Based Access Controls to Electronic Health Records

Laird A. Pisto

ABSTRACT: In the United States, personal privacy is considered a right. The exponential growth of stored data often is perceived as jeopardizing this right. Privacy concerns have resulted in health information legislation at state and federal levels. Healthcare organizations currently lack the capability to administer privacy-centric role-based access controls in strict compliance with these laws due to functional design limitations associated with existing information technology. Information is now funneled into systems from a wide range of sources, often with little or no accompanying information about the original source data. Government incentives promote increased sharing of electronic health records among providers, payers, and other healthcare organizations and their business associates, making compliance with patient privacy and security rules even more complex. Managing controlled access to electronic health records within many structures is increasingly difficult; therefore, healthcare attorneys need to understand their clients’ health information access control capabilities and advocate for programmed adaptations and enhancements to respond responsibly to these often competing goals for information sharing and patient privacy.

KEYWORDS: Role-Based Access Control, Privacy-Centric Role-Based Access Control, Purpose Binding, Decentralized Patient Data Repository


The author’s biography appears on the next page.
Laird A. Pisto is Associate General Counsel for MultiCare Health System, an integrated healthcare delivery system based in Tacoma, WA. He is co-chair of the American Health Lawyers Association Health Information Technology Electronic Health Records Affinity Group. Contact him via email at Laird.Pisto@multicare.org.

The author thanks Jake B. Kempton, a third-year law student at Seattle University School of Law, for his many efforts in organizing and editing this Comment.