# Assessing the other 'R' in RHIOs: Risk and liability of electronic privacy implications

By Cristian Lieneck, PhD, FACMPE, FACHE, FAHM

ACMPE Fellow

Regional Health Information Organizations (RHIOs) have developed at a rapid pace ever since the genesis of the Office of the National Coordinator for Health Information Technology (ONC) in 2004 as well as the legislative mandate for EHR adoption and meaningful use of such technology by the Health Information Technology and Clinical Health (HITECH) Act of 2009. With the intent of improving the health status of the population, this enhanced availability and exchange of health information creates an unavoidable risk for medical group practices at various levels within regional health information exchanges (HIEs).

**BASIC EXAMPLES OF PHI PATIENTS OFTEN REQUEST STRICT CONFIDENTIALITY**

Communicable diseases/diagnoses
*Example: HIV/AIDS, other sexually transmitted diseases*

Mental health treatment/diagnoses
*Example: psychotherapy notes, institutional treatment notes*

Addiction management/treatment
*Example: drug/alcohol treatment*

## Patient preferences

Each patient's medical record includes private information ranging from basic demographics to sensitive protected health information (PHI). It is common for a patient to inform one medical provider of a sensitive health detail and fail to disclose the same information to another provider.[1,2] The new capability of medical providers to exchange information on a single patient resolves this "failed omission" if the PHI is accessible via an HIE at either a local, state or regional RHIO level. Because of this layering of healthcare information platforms, PHI could travel several potential critical paths into another medical provider's hands, which might not have been the patient's preference.

The box above shows several common PHI examples of certain medical conditions that patients often do not want to share with all providers. Additionally, the figure (page 43) shows three basic routes (critical breaches) by which PHI could flow to a third-party medical provider using the HIE.

## Layers upon layers of responsibility

The HIE will not function effectively without the collaboration of multiple healthcare entities. As more providers adopt EHRs, demonstrate meaningful use and collaborate, responsibility for PHI becomes vague due to the number and levels of stakeholders participating in the system.[3,4] Although HIPAA controls the use of PHI in the course of medical practice, it was passed and enacted prior to the availability of EHRs and HIEs. Furthermore, the application of HIPAA privacy laws to HIE data use is limited and often difficult to interpret due to the nature of the HIE and HITECH's (2009) meaningful use incentives.[3]

So who is responsible for the security of this information? Referring back to the figure on page 43, is Provider B responsible for accessing inappropriate, unnecessary PHI information from the local/community HIE database, or should the HIE be held responsible for releasing it without proper authorization? The same question can be presented for breach 3. Provider B might commit breach 4, thus distributing the secure PHI information from Provider A's practice, either knowingly or unknowingly. This level of PHI transmission need not be conducted via meaningful use EHR/HIE but through standard medical records communication methods. Furthermore, as ONC continues to work toward a goal of full HIE integration for the nation, the access requirements and limitations that will exist beyond the state/RHIO levels remain unknown.

## Privacy preemption

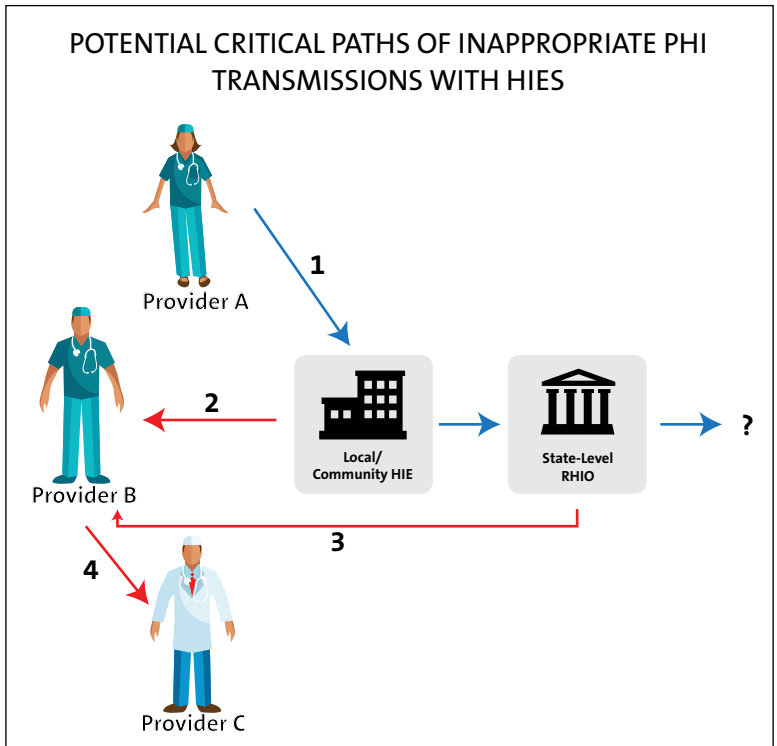
Currently, professionals in several states are discussing the wealth of PHI information housed in

HIE cloud systems, proper security access to the levels of each patient's information and "break the glass" procedures, which allow medical providers to enter secure areas of a patient's HIE medical record data during emergency situations. However, although EHR systems at the organizational level have allowed for behind-the-scenes forensic identification of medical record PHI breaches, this monitoring capability has not prevented inappropriate access to confidential PHI maintained in various cloud environments. Extreme cases of such electronic privacy breaches, both internal and external to the healthcare organization, have been thoroughly documented in the United States.[5,6,7] As state laws continue to expand federal PHI confidentiality regulations, practice professionals need to take preventive action to ensure that medical providers' and staff members' inappropriate access to confidential patient information is disallowed while using the HIE platform.

## Opt-in and opt-out consent models

Healthcare consumers who seek medical care within a regional HIE coverage area are often presented with opt-in or opt-out PHI consent forms that give them control over their electronic PHI at various levels. Although both models have advantages and disadvantages for the HIE, providers and patients, most EHRs and their corresponding HIEs are currently not able to delineate among selected PHI and a patient's mandate to not submit such information to the HIE against the information that is acceptable to share with the HIE.[3] Successful control over such PHI can be developed and enhanced once state and federal regulations dictate where the responsibility lies for any potential breach throughout the HIE pathway and the associated healthcare stakeholders involved with the PHI breach.

As a result, medical practices participating in HIEs should ensure that patients are blatantly aware of any EHR limitations and inabilities to refrain from submission of selected PHI information to the HIE and RHIO to avoid future privacy liability issues.




*Demonstration of the inappropriate flow of PHI through a standard local/ community HIE, a state-level RHIO and participating third-party exchange medical providers/organizations (non-emergent situation).*

Notes:

1. Talen M, Grampp K, Tucker A, Schultz J. What Physicians Want From Their Patients: Identifying What Makes Good Patient Communication. *Families, Systems, & Health*, 26(1). 2008.
2. Platt F. What Drives Doctors Crazy? *Families, Systems, & Health*, 26(1). 2008.
3. Fox SJ, Szabo DS, Burde HA. Managing Information Privacy & Information in Healthcare: RHIOs and HIPAA. HIMSS Privacy & Security Toolkit. 2007. Retrieved from: himss.org/files/HIMSSorg/content/files/D71_RHIO_Guidebook_HIPAA_Chapter.pdf.
4. Rosenfeld S, Koss S, Siler S. Privacy, Security and the Regional Health Information Organization. California HealthCare Foundation. 2007. Retrieved from: allhealth.org/briefingmaterials/chcf-rhioprivacy-1091.pdf.
5. HealthLeaders Media. Sutter Health Says Patient Data was Stolen. 2011. Retrieved from: healthleadersmedia.com/content/TEC-273422/Sutter-Health-says-patient-data-was-stolen.html.
6. Clark C. Six Major Patient Record Breaches Draw $675,000 in Penalties. 2010. Retrieved from: healthleadersmedia.com/page-1/LED-252360/Six-Major-Patient-Record-Breaches-Draw-675000-In-Penalties.
7. Monegain B. Breach into 'Octuplet Mom's' Medical Records Highlights Privacy Issues Again. 2008. Retrieved from: healthcareitnews.com/news/breach-octuplet-moms-medical-records-highlights-privacy-issues-again.

Read our feature story about HIEs in the May/June issue of MGMA *Connexion*. mgma.com/virtualconnexion.