

THE HITECH ACT – What Healthcare Organizations Need to Know about Access Compliance

By Brian Cleary

The Health Information Technology for Economic and Clinical Health Act (HITECH) evolves HIPAA from a reactive compliance requirement to a broader, more preventative approach. HITECH This act will impose more stringent regulatory and security requirements to the privacy rules of HIPAA, such as extending the covered entities to include business associates and related third party vendors in the healthcare industry, increased audit requirements, more proactive measures to protect personal healthcare information (PHI), increased civil penalties for a compliance violation of HIPAA, and stricter notification requirements of a security breaches of protected. Additionally, the HITECH Act authorizes state attorney generals to bring civil actions on behalf of state residents adversely affected or threatened by HIPAA violations of HIPAA.

With the dramatic increase of breaches and theft of PHR, the HITECH Act provides an opportunity for healthcare organizations and their partner networks to implement an information access governance framework in conjunction with modernizing how patient information is stored and accessed through electronic health records (EHR). From a trust perspective, the general public has significant concerns about the privacy of their PHI and may not want to have it accessed via EHR if they cannot be assured of the security of the information. Additionally, the increased audit requirements related to HITECH requires a system of record that can provide not only the evidence of compliance, but also the historical audit trail for who has access to, and who did access, EHR.

What impact will this have on organizations from an access governance perspective?

Computerizing patient health information will be fraught with risk if consideration around the access controls for EHR is not taken into account as part of the planning and rollout phase. As with many regulatory mandates, the specific control requirements in HIPAA and the HITECH Act are too vague and not clearly explained – which leaves far too much to interpretation. When thinking of implementing a set of preventative controls for accessing EHR, healthcare organizations must consider a governance framework that provides them with the visibility to who access to EHR information, how they got it, who authorized it and whether it is absolutely necessary as part of their functional role.

The foundation of any access governance initiative should be adherence to the principle of *least privileged access* or, as it is stated in HITECH, minimum necessary. This means that legitimate users should have no more access than the minimum required to do their job. Unacceptable access risks begin to appear when this principle is violated, and this type of violation takes place on a regular basis within many healthcare organizations.

Consider these findings from a recent Ponemon Institute surveyⁱ of IT security practitioners from U.S. business and governmental organizations:

- User access rights are poorly managed. Seventy-eight percent of respondents believe that individuals have too much access to information assets that are not pertinent to their job description.

- Policies are not regularly checked and enforced. Sixty-nine percent indicate that access policies within their organizations are either enforced poorly or not at all. Meanwhile, only 30% state that their organization makes sure user access policies are validated.
- Organizations are not able to keep pace with changes to users' roles and they face serious noncompliance and business risk as a result. Responses show that more than half (55%) describe their company's ability to grant access rights based on role and job function as poor or nonexistent, including 42% who report that it is not done at all.

¹ *2008 National Survey on Access Governance*, Ponemon Institute, February 2008

The failure to enforce the rule of least privileged access is often caused by entitlement inertia, which is the failure to remove previously issued access rights within an information resource once they are no longer necessary or appropriate. It is not unusual, for example, for employees, contractors, consultants and partners to accumulate unnecessary access privileges over time. The typical scenario happens when employees are promoted or transferred within an organization. Some of these entitlements (specific access rights to/or within an information resource) may become compliance violations over time or represent other security risks to a healthcare organization. If entitlements are not revoked when the relationship with the user is terminated, accounts will still be active in information systems that cannot be mapped to current users (which will create issues when external auditors check on controls. As a result, the systems can be accessed by an unauthorized user if they live outside the control of the network. This is a surprisingly common problem and it tends to be a consequence of the pressure put on IT security departments to provide access quickly when employees are transferred or promoted into positions that require access to new information resources.

Healthcare organizations that do not certify access on a regular basis and are not using a role-based approach for managing access change are most susceptible to this “entitlement creep” problem. In addition, many enterprises simply lack the ability to manage the constant change that occurs to functional roles across a large population of users to ensure that their access is appropriate for their new job responsibilities.

Extending the entity coverage:

Access governance must now extend beyond the internal healthcare network to covered entities and business associates to be able to demonstrate compliance with HIPAA under the HITECH Act's changes. Healthcare organizations need to be concerned about how effective the access controls are in their partner network. It's not just the expansion of entities and business associates under HITECH that healthcare organizations should be concerned with. With the amount of outsourcing of business processes and information systems that healthcare organizations have done in an effort to reduce operating expense, governance frameworks must be extended outside the enterprise. Don't rely on a SAS 70 report as a governance framework as it has failed in many cases to protect organizations from ultimate liability for compliance violation.

An effective approach for access governance should address:

Controls automation:

Organizations need to implement a set of automated controls for access delivery and change management that ensure policies are being applied in a consistent fashion and access related risk is avoided. A set of event-driven controls and processes need to be put into place that address change (joining, moving within or leaving) to a user's relationship with the organization.

Remediation & validation:

When change to a user's access is required, ensuring that the change request took effect (inclusion or deletion) is critical. Having an automated, closed-loop remediation and validation process will ensure that application owners and system administrators have executed on the access change request in a timely fashion.

Access review and certification:

Whatever the cause, organizations that do not certify access on a regular basis are most susceptible to "entitlement creep" and to prolonged exploitation by system intruders whose access, once established, goes unnoticed. Review and certification provide a set of detective controls that are typically required by many regulations and industry mandates such as SOX, PCI and HIPPA (to name a few). Access review also contributes to achieving the minimum required access principle as this process will provide business unit reviewing managers the ability to identify and remediate entitlements that are not required for a user's role within the organization.

Moving from detective to preventative controls:

The biggest challenge for most healthcare organizations is the ability to apply access policy controls in an environment of constant change to user relationships and roles. The complexity associated with managing the level change that most healthcare organization experience on a daily basis is where the breakdown in policy controls typically occurs. This is where using business roles to determine the access necessary for a functional or process role can help healthcare organizations better manage changes to access. Once business roles have been modeled with the appropriate access entitlements, if additional access is requested organizations can easily understand if it will create toxic combinations that introduce compliance or business risk by running their rules against the request.

Roles will simplify the change management process for the IT organization by first enabling individuals in the organization to request pre-determined, compliant roles, and secondly but ensuring a closed loop validation process that will ensure that entitlements not required for the new role are remediated. Leveraging a roles-based approach for governing user access governance will not only strengthen the policy framework by putting in place a set of preventative controls that operated at the point of request or change, it will also to streamline access delivery and ensure better accuracy for the access that is delivered. The access delivery efficiencies that can be realized by the IT organization alone can justify investing in this approach. When you consider having the ability to ensure that access control policies are enforced in a consistent fashion across the entire enterprise, access compliance and risk management objectives will automatically be realized and the complexity of managing access change will be dramatically reduced.

With such an access governance framework in place, healthcare organizations will be well on their way to managing the business and regulatory risks of inappropriate access to its information resources. The right solution requires a strategic approach to access governance

based on auditable business processes that provide complete visibility and accountability for user access.

Brian Cleary is senior vice president of products and marketing for [Aveksa](#), the market-leading provider of enterprise access governance solutions.
