e-volve Information Technology Services

Municipal & Enterprise Information Technology Services

Information & IT Governance Information Security & Cybersecurity

Audits and Assessments • Strategic Planning • Enterprise Software Procurement • Business Process Reengineering
Project & Implementation Management • Regulatory Compliance • IT Service Management • Virtual CIO

e-mail: jmorgan@e-volvellc.com
Phone: (607) 731.4097

HIPAA as a framework for county/municipal cybersecurity

Are you a covered entity?

Basing a county/municipal Information Security (InfoSec) & cyber security framework on HIPAA is a logical choice if some part of your organization is a covered entity (CE) under HIPAA.

How do you know if you are a CE? If some department or division within your organization is a Health Care Provider, Health Plan, or Healthcare Clearinghouse, they are a CE. If you have clinics, doctors, psychologists, clinical social workers, chiropractors, nursing homes, or pharmacies, you are a CE[i]. Moreover, many counties have divisions or departments that function as Accountable Care Organizations (ACO), Managed Care Organizations (MCO), Healthcare Clearing Houses, or Health Maintenance Organizations (HMO). These are all common functions, especially within large county governments.

Are you in compliance?

If anything described above applies to your county or municipal organization, one or more divisions of your organization is a CE and is required to be in compliance with both the HIPAA Security Rule and the HIPAA Privacy Rule. In my experience, most county governments that have covered entities are out of compliance. Where does your organization stand?

I suspect what often happens is that executives look at something like information security policy requirements and say:

> *This has tech words in it. IT handles tech stuff. Therefore, I'll turn it over to IT to handle.*

What a huge mistake. Organizational policy dealing with the manner in which information is handled, regardless of whether or not HIPAA regulations apply, requires communication and coordination with Legal, HR, IT, Information Security, Risk Management, Archives, County Clerks, and other divisions within your organization. It's not a tech issue; it's a high level, interdisciplinary executive function. It is an Information Governance (IG) issue and it shouldn't be handed off to your IT Director or CIO to address unilaterally.

There are a number of reasons why IT should not be delegated sole responsibility for organizational information security. For one, a successful information security program requires overlapping layers, checks, balances and oversight. ***Trust but verify!***

A successful program also requires expert knowledge of departmental business processes that often exceeds the knowledge of the IT staff. Moreover, if your department heads have equivalent status within the organization, it is not appropriate for a CIO or IT Director to unilaterally dictate policy to his or her colleagues of equal status. There are far too many IT Departments that have adversarial relations with their end users because of their autocratic and often illogical decrees. Information security requires a team approach with executive and board oversight.

Extend HIPAA to your enterprise

If you have covered entities in your organization and have limited or nonexistent enterprise security policies, I recommend that you consider building your entire enterprise information security policy on the HIPAA Security Rule in order to raise the entire organization up to that that level while also getting compliant with federal law.

Why? It is highly probable that your organization uses shared facilities, shared IT infrastructure, and shared services. Multiple information security levels create a significant management challenge and are certain to cause chaos and confusion. Multiple security stances will lead to security gaps and ultimately to breaches. Keep it simple and operate at the highest standard using generally accepted, good practices.

e-volve Information Technology Services
Municipal & Enterprise Information Technology Services

Information & IT Governance Information Security & Cybersecurity

Audits and Assessments • Strategic Planning • Enterprise Software Procurement • Business Process Reengineering
Project & Implementation Management • Regulatory Compliance • IT Service Management • Virtual CIO

e-mail: jmorgan@e-volvellc.com
Phone: (607) 731.4097

Someone is surely hollering, "Jeff, we also have CJIS (Criminal Justice Information Systems) to comply with in law enforcement. What about that?" We'll leave CJIS compliance for another day – but that represents another area of risk, limited understanding, and questionable compliance in municipal government agencies.

Develop your policy with the HIPAA Security Rule

There are two major components to HIPAA, the Privacy Rule and the Security Rule. For the purpose of this discussion, only the Security Rule matters, but we'll definitely discuss privacy another day.

The original document, *45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule* is 49 pages of small print. However, the meat of the document is contained within the final six pages and includes a handy matrix on page 48 (8380 of the federal register).

The security standards in HIPAA are broken down into three sections, each of which has multiple layers and sub components:

- Administrative Safeguards (9 components)
- Physical Safeguards (4 components)
- Technical Safeguards (5 components)

These three major areas break down into at least 43 separate policy areas where your organization must build safeguards including risk analysis, contingency planning, backup, passwords, HR sanctions and terminations, disaster recovery, encryption and many more.

Using the components in the matrix should enable you and your IG committee to quickly generate a suite of security policies that, when implemented and enforced, will vastly improve your current information security stance.

These are all policy areas that must be addressed as a matter of good practice whether or not you are a covered entity. This is why HIPAA is an excellent starting point for municipal governments that are InfoSec policy deficient.

Next Steps

1. Find out where your organization stands in terms of information security policies and procedures.
2. Find out whether or not you have covered entities in your organizations. Must you comply with HIPAA? Are you compliant?
3. Meet with your IG committee to discuss your findings.
4. If you don't have an IG committee – get one started.
5. Download and review the HIPAA Security Rule. Use it to build your organization's information security policies.
6. Use PDCA (Plan, Do, Check, Act) or DMAIC (Define, Measure, Analyze, Improve, Control) to maintain continuous improvement.
7. Begin building a culture of security in your organization.

More Information

If you would like to discuss information security in your organization, e-mail me at jmorgan@e-volvellc.com.

This article first appeared on CIO.com at http://www.cio.com/article/3188667/governance/hipaa-as-an-umbrella-for-countymunicipal-cybersecurity.html

References

[i] US Department of Health and Human Services. Covered Entities and Business Associates.