HIPAA Regulatory Alert
Cutting-edge information on privacy regulations

Going too far with HIPAA compliance threatens care provided to patients

Overzealous individuals can become the 'HIPAA police'

Healthcare providers have spent years grappling with how to comply with the Health Insurance Portability and Accountability Act (HIPAA), with most of the focus on training clinicians and staff about the dangers of too freely providing protected health information (PHI). Now a new worry is emerging as some providers take HIPAA compliance too far and threaten patient care.

A recent report from the Bipartisan Policy Center, a think tank in Washington, DC, raised the alarm that HIPAA is too far-reaching and "often misunderstood, misapplied and over-applied in ways that may inhibit information sharing unnecessarily." *(See the story on p. 3 for more on that report.)*

The problem can occur in many healthcare settings, but the IT department is a common source. Some hospital IT departments see themselves as "the HIPAA police" and clamp down in ways that HIPAA doesn't require, says **Abraham Gutman**, CEO of AG Mednet, a Boston-based company that assists providers with communication of clinical trial data. Gutman specializes in the de-identification of patient information specific to clinical trials, and he says that with everyone acting as a judge of what HIPAA requires, clinical research and patient care are impeded.

IT departments should publish guidelines on proper HIPAA interpretation to encourage collaboration instead limiting it out of fear, he suggests. The guidelines should explain what is possible in moving data, rather than only focusing on what is prohibited. Explain clearly what safeguards, such as encryption or de-identification, are necessary so that IT managers are willing to try to say "yes" instead of automatically saying "no."

"In my experience the IT departments are among the least knowledgeable about how to comply with HIPAA, but what they do understand is that a breach traced back to them would have very severe consequences," Gutman explains. "Consequently they take the most conservative approach. Nothing can get out, and nothing can get in."

The IT department, however, is sometimes seen by others as authoritative on HIPAA because it is in charge of data transfer. In that case, the IT department's overreaction is passed on to other departments and individuals, eventually creating a culture in the organization that is not based on an accurate HIPAA interpretation but nonetheless hinders data sharing, Gutman explains. *(See the story on p. 3 for an explanation of how the IT department might capitalize on confusion over HIPAA compliance.)*

"It hinders through fear. There is so much fear among the doctor and nurse population that people don't even ask if they can move some data," Gutman says. "They assume from past experience that the exchange will never be approved, so they might as well not ask."

Educate rather than scaring employees

Risk managers, compliance officers, and other administrators should consider whether they are merely scaring employees about HIPAA violations or educating them about the true spirit of the law, suggests **Stephen Cobb**, senior security researcher with ESET, a company based in San Diego that provides IT security for healthcare providers. HIPAA was never intended to prohibit valid data exchanges, but years of scare tactics have made employees fearful, he says.

"What we have ended up with, unfortunately, is a system of compliance that is diametrically opposed to the idea of providing healthcare," Cobb says. "There are some threats to healthcare data, but most of the information threats are for general information rather than people seeking out healthcare data in particular," he says.

Cobb says he is sympathetic with healthcare IT professionals who may be too strict, because they tend to be on the leading edge of understanding what threats exist and how to resist them. Limiting access to data is always key, so he advises working closely with IT staff to develop reasonable policies. "You have to find a way to rein them in if they are going too far, but without diminishing their enthusiasm for security," Cobb says.

Institutions can be guilty of writing HIPAA policies that are overly strict, but more often the problem lies with individuals who do not know the policies or are overzealous in their interpretation, Gutman says. In particular, employees should be reminded that the patient