

Sponsored by:

# NETWORKWORLD

This story appeared on Network World at  
<http://www.networkworld.com/research/2005/053005-jail.html>

Feature

## Worst-case scenario

By [Paul McNamara](#), *Network World*, 05/30/05

Prison? ... An IT guy? ... For violating [HIPAA or Sarbanes-Oxley](#) ? ...

Could it really happen?

It's known as the "go-to-jail scenario" in IT circles, a confluence of events that might land a CIO or network executive not just in hot water, but behind bars. You've probably heard loose talk about this risk at industry conferences and in the press. But can an IT exec actually end up doing hard time - as opposed to being fired or fined - for violating one of these federal laws?

The jury is still out. Everyone we talked to pretty much agrees that the go-to-jail scenario is a long shot that would require overt bad deeds far beyond simply screwing up. But no one was willing to entirely rule out the possibility of a stretch in the slammer, either.

Clearly, the legislation and regulations governing the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act and the like include criminal penalties: up to 10 years in prison with HIPAA for "obtaining or disclosing protected health information;" 10 to 20 years with SOX for "destruction, alteration or falsification of records," just to cite two examples.

And a former cancer clinic worker in Seattle became the first person convicted of criminal charges under HIPAA last November. The sentence: 16 months for using patient information to fraudulently obtain credit cards. Experts say this case isn't all that instructive in terms of how these laws will be applied toward IT executives because this type of outright fraud has always carried the threat of prison.

But the reality is that more IT professionals are finding themselves in the enforcement cross hairs.

"There's no question that more and more people from the IT world are becoming responsible for electronic records management," says Bob Williams, president of Cohasset Associates, a Chicago consulting firm that specializes in document management. Primary responsibility for electronic records management rests with IT in more than 70% of organizations, according to a Cohasset Associates survey of 2,200 records-management professionals. And with that primary responsibility comes vulnerability to enforcement penalties.

"Clearly Sarbanes-Oxley holds out prison as a possibility, but I think that it is more likely to occur for senior management than even a CIO," says Williams. That "more likely" is the type of caveat that experts sprinkle throughout their ruminations on this subject, which may or may not lend comfort to IT professionals who find themselves in a compliance-related crossfire.

"Maybe we should say it backwards: Can you definitively say an IT person would not go to jail?" says Jonathan Redgrave, an attorney with the Washington office of Jones Day, who specializes in electronic records issues. "You can't say that they wouldn't; it really depends on the facts of the situation."

The U.S. Department of Justice, which is charged with assessing alleged HIPAA violations sent to it from the Office for Civil Rights within the Department of Health and Human Services, couldn't provide much in the way of clarification.

If the Justice Department agrees that a HIPAA complaint warrants criminal prosecution, it will forward the case to the U.S. Attorneys Office nearest the infraction. "It is a case-by-case basis, and the scrutiny has to be made on each and every one to determine whether the government is going to prosecute," says Charles Miller, a spokesman for the Justice Department. As for hypothetical situations involving IT personnel, the government cannot offer blanket assurances about avoiding jail, he says.

## **Where there's a will ...**

Willfulness of action would likely be a key component weighed by any enforcement authority, Redgrave says, and if an IT person was found to be a willing participant in any attempt to illegally access, delete or cover up protected records it is more likely that criminal penalties would apply. Simply doing a lousy job isn't likely to land one in jail, he says.

"Where you get the criminality is with obstruction of justice, like the Arthur Anderson situation,"

### **HIPAA CRIMINAL PENALTIES**

Any person who knowingly obtains or discloses individually identifiable health information in violation of the Administrative Simplification Regulations faces a fine of up to \$50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a \$100,000 fine, and up to five years in prison. Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of \$250,000, and imprisonment for up to 10 years.

Redgrave says. "Let's say you are someone in the IT department at Arthur Anderson and you decide it's a good idea - even though you know the SEC is coming - to allow purges to take place or press the system operator to have the purge take place: You're getting closer to a problem."

**SARBANES-Oxley: Sec. 1519. DESTRUCTION, ALTERATION OR FALSIFICATION OF RECORDS IN FEDERAL INVESTIGATIONS AND BANKRUPTCY**

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies or makes a false entry in any record, document or tangible object with the intent to impede, obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

Craig Rhinehart, director of compliance markets and products at FileNet, sees the threat in more cut-and-dried terms. "Yes, IT professionals can go to jail," he says. According to Rhinehart, the challenge for IT professionals will be balancing the immediate risk - an agitated boss at their door right this moment - against the future risk of being held accountable for a compliance violation that may carry criminal penalties.

"Some senior manager comes to an IT administrator and says 'I need to have access to these files.' If you give him access, you may have just become an accomplice to a crime," Rhinehart says. "You can't tell me that most mid-level or even senior IT managers [won't acquiesce] if the CEO or CFO comes marching into their office and says they need to check on a few things."

The key to avoiding that scenario is a clear set of policies and procedures for managing any information that might be subject to corporate governance laws or litigation, Rhinehart says. "If not, you leave the interpretation up to the individual and that's where trouble starts," he says. "If there's no clear policy in place you might be doing something that is technically illegal." You also might have a harder time fending off the executive who is demanding access to a particular set of records.

The bottom line is that preparation beats complacency, Redgrave says. "People talk about this and while it's not an everyday occurrence, there certainly is an element of risk such that the people involved really need to understand what they're doing."

All contents copyright 1995-2005 Network World, Inc. <http://www.networkworld.com>