

How healthcare providers are missing opportunities to ensure that investments in security and privacy are also lowering risks*

The Global State of Information Security 2007

43%

Percentage of provider respondents whose organizations do not require employees to complete training on privacy policies and practices.

1 out of 3

Number of provider respondents (34%) who say their organization keeps an inventory of third parties using patient data.

78%

Percentage of provider respondents who are not “very confident” in the effectiveness of their organization’s information security activities.

1:1

Ratio between the number of provider respondents who report their organization has security procedures that partners must follow and the number who report it does not.

It’s a crucial question—whether it’s asked by a hospital oversight board, a health system CEO, or attorneys supporting a network of physician practices. Now that the initial deadlines for complying with HIPAA have passed, have the enormous investments in protecting patient privacy also been effective at reducing other security-related risks to information, operations and performance? Absolutely. That’s the conclusion you might draw if you quickly scanned the spectrum of provider responses to the world’s largest survey on privacy and information security practices, the Global State of Information Security 2007. After all, the sector is far more likely this year to hire a Chief Privacy Officer (49% vs. 36%), post privacy policies on internal websites (71% vs. 56%), and require employees to certify in writing that they are complying with privacy policies (65% vs. 59%).

But a closer review would reveal the gaps—some of them critical and a few unexpected. For example, 26% of health provider respondents report their organization needs to be in compliance with HIPAA and is not. And almost 40% do not yet have an overall security strategy in place. We believe provider attention to several key areas would go a long way toward lowering risks and getting better business value from compliance-driven investments.

- **Dedicating more resources to protecting data is becoming an increasingly strategic priority.** Though providers encrypt data in transmission more frequently than organizations in other industries (67% vs. 61%, the cross-industry average), they are often much less likely to protect data at rest—in databases (39% vs. 50%), file shares (29% vs. 36%), and laptops (37% vs. 42%). At the same time, nearly two out of three providers do not have accurate inventories of which user data they keep (62%) or which locations and jurisdictions store this information (63%).
- **Investment returns will be much clearer when compliance practices become more tightly aligned with broader risk management objectives.** A clear majority of providers do not conduct a risk assessment either annually or semi-annually (65%)—a rate notably higher than payers (43%). Providers are also almost twice as likely as payers not to classify data and information assets by risk level (36% vs. 19%). Boosting investment returns, however, will require integration. Today only half of all providers (48%) link security, either through organizational structure or policy, to privacy and/or regulatory compliance.

Survey Methodology

The State of Information Security 2007, a worldwide security survey by PricewaterhouseCoopers and CIO Magazine, was conducted online from March 6 to May 4, 2007. Readers of CIO Magazine and clients of PricewaterhouseCoopers from around the globe were invited via email to take the survey. The results discussed in this report are based on the responses of 7,200 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries. The margin of error is $\pm 1\%$.

Of the 266 respondents from the healthcare provider sector, 66% were from North America, 18% from Europe, 9% from Asia and 7% from South America. Thirty percent (30%) reported annual revenues of at least \$500 million.

To learn more about the survey, or about how PwC helps companies address security and privacy issues, visit: www.pwc.com/gjss2007 or contact:

Mark Lobel
646 471 5731
mark.a.lobel@us.pwc.com

Daniel Garrett
276 330 8202
daniel.garrett@us.pwc.com

Robert Dondero
214 754 7448
robert.c.dondero@us.pwc.com

- **Security and privacy policies and practices are only valuable if they work.** Uncertainty about the business value of compliance investments will be high as long as providers are not checking up to see whether safeguards are actually being followed—or are even working. Most providers (61%), however, do not audit or monitor user compliance with policies and 55% have not measured and reviewed the effectiveness of security policies and procedures in the past year. Many administrators will also need to decide whether internal compliance can be achieved merely through improvements in training and awareness. Though writing rules is perhaps the most cost-effective security practice, two of the elements least likely to be included in health provider security policies include the collection of security metrics (26% vs. 45% reported by payers) and enforcement mechanisms (33% vs. 52% reported by payers).
- **The “insider threat” may actually be growing.** This year, 57% of provider respondents report that employees represented the most probable source of security incidents—a percentage higher than the cross-industry average (48%) and significantly higher than levels reported by payer respondents (36%). Has the “insider threat” truly increased—or are provider organizations simply more aware of the threat? It isn’t clear. But provider respondents identified the primary method of attack as the abuse of valid user accounts and permissions. In spite of this, barely a third of all provider respondents (36%) say their organization has tiered authentication levels based on user risk classification. Arguably, hospitals, among other providers, face the greatest “insider” challenge. With so many personnel—from doctors to nurses and technicians—logging into common stations, multiple log-on procedures quickly undermine the quality of patient care. In spite of this, only 22% of provider respondents report their organization has reduced/single sign-on software in place.

Security benchmarks: Healthcare (Percentage of responses from healthcare vs. other industries)	Health/ Provider 2007	Health/ Payor 2007	Pharma/ Life Sciences 2007	Financial Services 2007	All Industries 2007
Have an overall security strategy	61%	79%	58%	71%	57%
Engage both business and IT decision-makers in addressing information security	58%	80%	51%	64%	52%
Ensure that security policies include risk assessment	47%	71%	56%	62%	43%
Have a centralized security information management process	51%	57%	50%	57%	44%
Conduct compliance testing	41%	55%	53%	59%	40%

© 2007 PricewaterhouseCoopers LLP. All rights reserved. “PricewaterhouseCoopers” refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. SJ-08-0018-A 08-07 DB



**Business
Technology
Leadership**

