



By Mark L. Mattioli, Nicholas S. Gaudiosi and D. Scott Jones

Healthcare providers and their Professional Medical Liability (PML) insurers face a unique nexus of medical malpractice litigation and government regulation. Going back to the 1980s, Medicare fraud and abuse enforcement has been a priority for the government, and it moved to the privacy arena with the enactment of the Health Insurance Portability and Accountability Act (HIPAA) in 1996.

Further, the current impetus to enact healthcare reform has created new quality of care initiatives at the federal and state levels. For example, the Office of Inspector General (OIG) of the Department of Health and Human Services (DHHS) 2011 Work Plan calls for the OIG to reduce fraud, waste, and

abuse, and improve program efficiency and effectiveness. The goal of these initiatives is to improve the quality of healthcare delivery.

As a result of the efforts of the OIG and other federal investigative agencies, physicians and other healthcare professionals are under increased scrutiny not only for billing, but also for quality of care and medical necessity issues.

In one recent investigation, a Maryland interventional cardiologist and a hospital catheterization laboratory were investigated by the OIG for lack of medical necessity in the placement of stents, small devices designed to hold open arteries to the heart. In an attempt to be cooperative with investigators, the hospital sent letters to approximately 600 patients notifying them of the investigation.

Plaintiffs' counsel began aggressive media-based recruitment of these patients, resulting in hundreds of medical malpractice suits filed against the physician and hospital. This single example clearly illustrates the connection between quality and compliance investigations and medical liability.

Recovery Audit Contractors and Post Payment Audits

Effective January 1, 2010, the government expanded the role of Recovery Audit Contractors (RACs) to enforce billing compliance nationwide. In the implementation phase of the RAC program, more than \$1.3 billion of improper Medicare payments were found in five states. On a national level, the government is expecting to find over \$900 billion of improper payments. The RAC program is the most

aggressive measure taken to date by the U.S. government to find and prevent waste, fraud and abuse in medical billing, and recoup monies associated with abusive activities. Audit contractors retain 9 to 12 percent of payments recovered for the government.

RAC audits target both intentional and unintentional overbilling and can result in costly fines, penalties and restitution charges. RAC auditors are authorized to audit any and all fee-for-service providers. Accordingly, any medical practice with a Medicare provider number is subject to a RAC audit. In addition to RAC audits are the relatively new Zone Program Integrity Contractors that expand the government's audit capacity to providers not covered by the RAC audits. The auditors are independent contractors who have a work agreement with the government.

RAC and other provider audits are public investigations, and documentation of the investigation results and reports are available to plaintiff's counsel who understand how to mine federal Internet sites for data. This can create a pool of information easily used to recruit plaintiffs.

The significance is that if there is a finding of potentially fraudulent conduct, the matter can be referred to the United States Department of Justice for criminal prosecution or potential civil litigation under the False Claims Act. This litigation is extremely costly, and the fines have been described as draconian — \$5,500 to \$11,000 per claim in addition to treble damages. Given that these matters often involve hundreds, if not thousands of claims, the

fines can be astronomical. In addition to the government, private parties are authorized to bring suit in the name of the government (called *qui tam* actions) and collect a portion of any settlement or judgment recovered. The amount of such recovery depends on whether the government intervenes in the lawsuit. Such actions are filed under seal, and could be pending for some time until the complaint is unsealed. Thus, a provider may have little knowledge that a *qui tam* suit has been instituted.

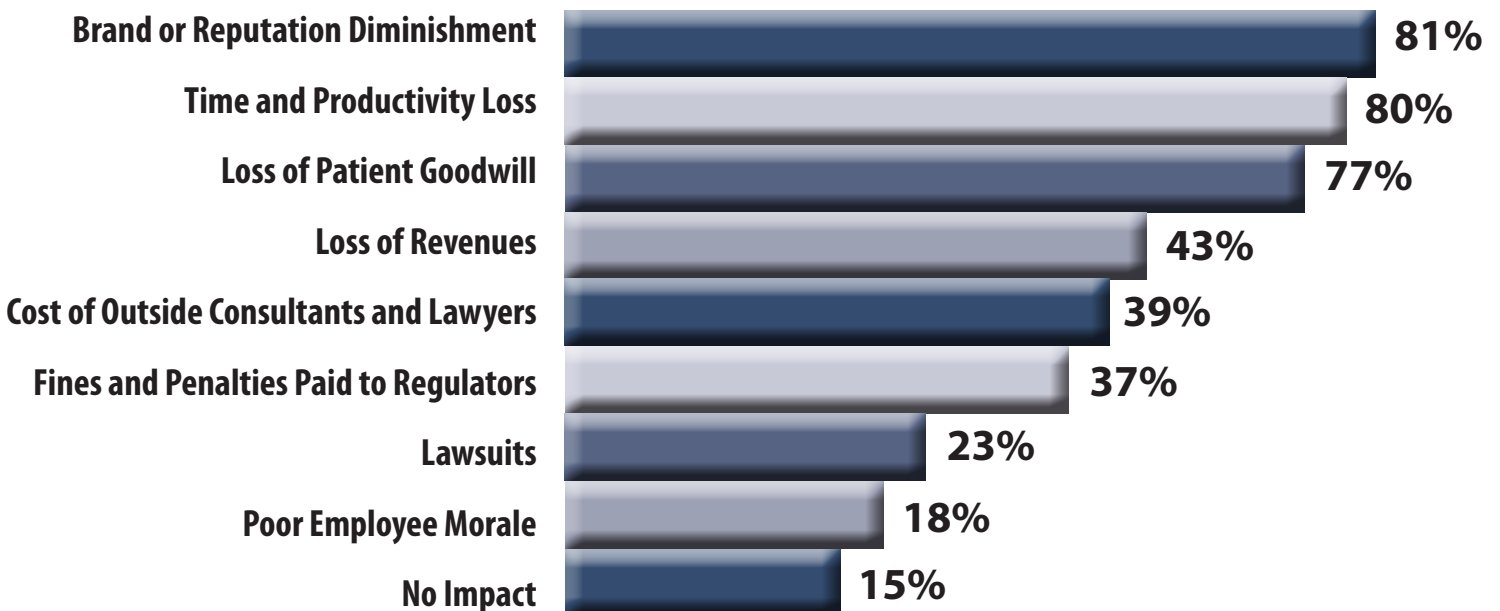
The Loss of Patient Health Information

Risk for healthcare providers and PML companies does not stop with federal or state investigations of billing and quality of care. The HITECH Act redefines federal guidelines associated with the loss of patient health information, making fines and penalties for data breaches more severe, and the procedures for remediation more onerous.

Under the Act, negligent compliance practices can result in fines up to \$1.5 million per incident. Healthcare providers are required to implement technical, physical and administrative safeguards of HIPAA's data security rules, and are permitted to use and disclose personal health information only as allowed by HIPAA's privacy rules.

Violators of these requirements are subject to civil and criminal penalties. In addition, HITECH mandates the steps that providers must take once a breach has occurred. In addition to fines and fees, the organization must conduct patient identity monitoring, internal cyber investigations and notification to affected individuals.

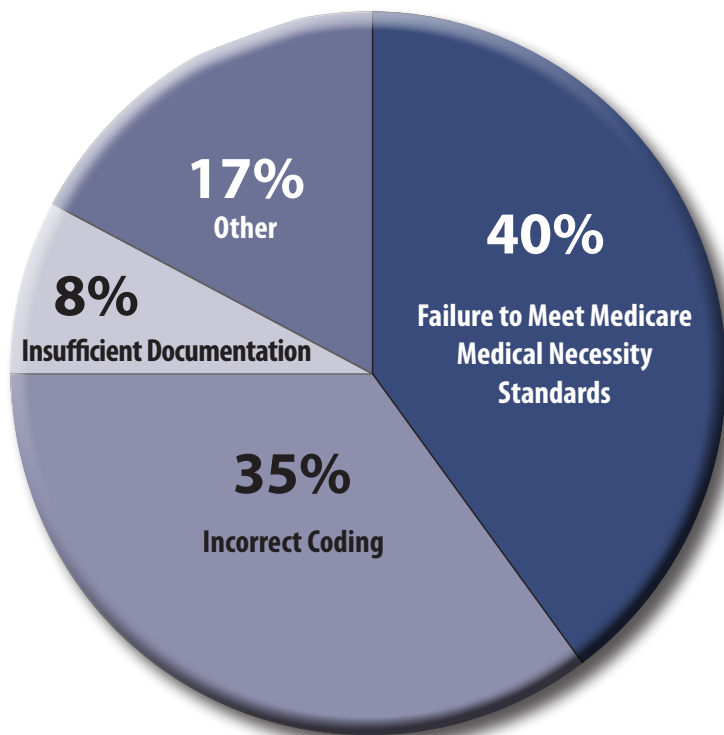
The Impact of a Data Breach on Medical Practices



Results of a 2010 Ponemon Institute Survey (Practices could indicate more than one response)

Ponemon Institute, LLC. "Benchmark Study On Patient Privacy and Data Security." Ponemon Institute© Research Report (November 9, 2010)

Reasons for RAC Overbilling Determinations



Source: AHA (November 2010). RACTrac Survey

A recent study done by the Ponemon Institute found that the average economic impact of data breach incidents over a two-year period is approximately \$2 million to the organization involved. Enforcement provisions of the HITECH Act are stronger than those found in HIPPA. In addition to possible criminal penalties, civil penalties under the HITECH Act can range from \$100 to \$50,000 per violation.

As medical practices rush to implement Electronic Medical Record (EMR) or Electronic Health Record (EHR) systems, the potential to expose patient information to loss increases exponentially. More importantly, adoption of EMRs and EHRs is almost mandated by HITECH, which provides significant incentives for users of such systems and penalizes those providers who do not utilize such systems. Further, provider efforts towards increased integration of services through such things as accountable care organizations will further drive utilization and sharing of robust electronic systems, thereby increasing the likelihood of a potential breach.

In addition to governmental enforcement actions, private plaintiffs have brought suit for breach of patient privacy. Accordingly, any breach must be managed to expect governmental and private enforcement actions.

Insuring Compliance

The federal focus on improving quality of care through audits and investigations is indisputable. Medical practices and health organizations are exposed to new risks and potential for loss under new audit programs. In addition, health information privacy regulations provide new types of risk exposures for providers of care.

Some innovative insurers are establishing new insurance programs that address these risk exposures and offer protections to physicians and their organizations. The significance is that having coverage for such claims at the initial level allows the provider to risk manage the situation so as to avoid the potential for collateral litigation after the initial investigation. This is especially true of the RAC and ZPIC audits, which could lead to very costly litigation under the Federal False Claims Act. Given the penalties, it is not surprising that few claims are actually litigated in the healthcare area. Even if the government decides not to go after the provider, there is still the threat from *qui tam* relators.

Looking Ahead

Healthcare providers and their insurers face new risk exposures. Investigations will focus on high-utilization, high-cost services rendered by medical specialists and specialty programs. Publication of investigative reports will provide the plaintiffs' bar with a ready source of new claims, which may involve medical malpractice and fraud.

New audit programs such as the RAC, will investigate providers at every level. As with public investigations, audit activities are considered public events that can be accessed by those interested in conducting research.

Healthcare providers and organizations seeking to protect themselves against these new exposures are demanding new partnerships and products from their insurers. Few traditional insurers appreciate the growing exposures created by the nexus of regulatory compliance, quality of care and medical malpractice. Nevertheless, addressing such issues at the early levels is key to preventing them from becoming costly litigation. [LM](#)

Mark L. Mattioli is Chair of the Health Law Practice Group for Marshall, Dennehey, Warner, Coleman and Goggin, King of Prussia, Pa. Nicholas S. Gaudiosi is Senior Vice President & Chief Operating Officer and D. Scott Jones, CHC, is Senior Vice President, Claims and Risk Management of HPIX, which is an insurance exchange providing services to physicians and providers in the Mid-Atlantic region.