Over $5 million in Health Insurance Portability and Accountability Act (HIPAA) penalties were levied in February 2011; these scenarios provide us the opportunity to explore the potential for other financial exposure arising out of HIPAA.

Cignet Health Center has the dubious honor of being assessed the first HIPAA Civil Monetary Penalty imposed since the rule took effect in 2003 yet it only took days for the second settlement, against Massachusetts General Hospital, to follow.

HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH) provide a set of federal standards to protect an individual’s Personal Health Information (PHI) while being maintained by covered entities: health care providers including doctors and pharmacies; health plans including Medicare and Medicaid; and health care clearinghouses. HIPAA HITECH is enforced by the US Department of Health and Human Services Office of Civil Rights (OCR).

Cignet Health was fined $4.3m for denying 41 patients access to their records and subsequently refusing to cooperate with the investigations. It has been argued that Cignet's fine could have been even higher, but for a calendar year limit of $1.5 Million per violation.

Mass General was fined $1m by the OCR for a 2009 data breach caused by employee who left on a subway documents containing PHI & billing information of 192 individuals including patients with HIV/AIDS.

Expect to see more HIPPA fines and settlements from the OCR. In their recently published 2012 Justification of Estimates for Appropriations Committees they've petitioned for an increased budget to fund their enforcement objectives.

The February HIPAA fines have grabbed headlines, but a covered entities’ financial exposure does not end there.

Notification Costs
HIPAA mandates covered entities notify each affected individual (non-covered entities must comply with state law notification requirements). Both Cignet & Mass General would therefore incur direct, calculable costs to identify, locate and notify the data subjects. Notice must also be provided to the Secretary of the US Department of Health and Human Services and in some circumstances, to the media.

Defense Costs & Additional Liability
State Attorney General
HITECH empowers state attorneys general to bring civil actions. The first of such actions was announced on 6 July, 2010 when Connecticut Attorney General settled with Health Net for losing a disk containing health and other private information of 2m people, 500k of whom were Connecticut residents.

The Connecticut settlement includes statutory damages of $250k, mandatory corrective action, consumer credit monitoring & identity theft insurance, and reimbursement for the costs of security freezes. Under the settlement, Health Net and its affiliates also agreed to an additional contingent payment to the state of $500,000, should it be established that personal information used illegally, impacting plan members.

Reputation
Cignet is a private medial and Health Plan, their failures in this case could cost them in terms of lost existing and/or new enrollees

Other Privacy Laws
HIPAA will take precedence over any contrary state law unless the state law is more stringent than federal law (or a specific exception applies), we have otherwise found no support for the idea that liability under one statute would pre-empt other Privacy Laws.

In the Mass General example, the exposed sensitive personal information resulted in a call for a class action for emotional distress arising from invasion of privacy. It’s conceivable that the exposed billing information could also result in Identity Fraud claims, which though difficult to prove can still impose hefty defence expenses.

When Cignet eventually provided regulators with the requested information, it also included records for 4,500 individuals that were not subject to the order. Cignet had ”no basis for the disclosure” of those patient's records, which could trigger yet more obligations.

Before they started fining violators in February, the OCR had previously imposed significant civil liability for willful violations of the Privacy Rules which they sometimes investigate along with the Federal Trade Commission (FTC):

- 2010 Rite-Aid: $1m settlement of a joint investigation for improper disposal of PHI.
- 2009 CVS Caremark: $2.5m settlement for improper disposal of PHI.
- 2008 Providence Health & Services: $100,000 settlement amount to the OCR

Compliance
Each of the above covered entities found that settlements with either Agency can result in long term, expensive corrective action plans. The cost for these measures must be borne by the covered entity.

To settle with the FTC an entity may be required to establish a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from consumers and employees. It also requires the company to obtain, for a period up to 20 years, an audit from a qualified, independent, third-party professional to ensure that its security program meets the standards of the order.

The OCR can also require corrective measures such as improving internal policies & procedures regarding physical and technical safeguards (e.g., encryption), governing off-site transport and storage of electronic media containing patient information; workforce training on the safeguards; conducting audits and site visits of facilities; and submitting compliance reports to OCR for a period of three years.

A Cyber/privacy insurance policy with an insurer at Lloyds of London could provide possible coverage for Cignet, Massachusetts General, Rite-Aid, CVS & Provident Health as follows:

- Civil fines & penalties and costs to defend a regulatory action arising out of a breach of privacy or confidentiality.
- Legal/consultative expense to ensure the extent & content of notification required, i.e. federal pre-emption or state notice required?
- Direct costs to comply with mandatory notification & credit monitoring. Ponemon estimates the cost to notify is $90 per affected customer.
- Indirect costs of a privacy event (abnormal loss of income or lost customers), again according to Ponemon, is an additional $114 per affected customer.
- Defense and settlement of privacy liability claims.

http://www.boston.com/news/local/massachusetts/articles/2009/05/21/hiv_patients_sue_after_records_lost/
For more information on a Cyber insurance policy for a broker dealers or investment advisors, please give us a call.

Lyndsey Bauer
Senior Vice President
t: (011) (44) 20 7280 8228
e: lbauer@paragonbrokers.com

Tom Quy
Cyber Liability Broker
t: (011) (44) 20 7280 8252
e: tquy@paragonbrokers.com