



MEMORANDUM

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

To David Watkins

FROM Philip D. Porter
Timothy P. Tobin

TELEPHONE 1.703.610.6108
1.202.637.6833

DATE November 18, 2010

SUBJECT ISO 27001 Certification

Companies, including those in the insurance industry, inevitably maintain not only sensitive confidential information about their business processes and pricing, but also personally identifiable information that federal and state laws and regulations, and in some cases local laws and regulations, obligate these companies to protect. The broadest definitions of personally identifiable information include an individual's name and only one other item of related information, such as residence address, telephone number, social security number or drivers license number. Companies that engage other companies to perform data processing and other back-office services routinely impose confidentiality, privacy and data security obligations on these service providers. A service provider's breach of any of these obligations can expose the company to a public relations debacle, lawsuits, and in the event of loss of personally identifiable information, fines, penalties and notification expenses.

Any company that makes its confidential information available to a service provider should assure itself that the service provider can keep the company's confidential information safe and secure, i.e., that the service provider has adopted specific business processes that are designed to protect its clients' confidential information. Obtaining satisfactory assurances is voluntary and in a company's own business interests for purposes of confidential business information. By contrast, however, federal and state privacy and data security laws and regulations obligate a company that collects personally identifiable information to make that information available only to service providers that have in place a reasonable, comprehensive information security program that includes physical, technical and administrative safeguards for handling personal information.

Data protection requirements at the federal level include:

- the Gramm Leach Bliley Act (GLBA) specifies data security requirements for personal financial information handled by financial institutions;
- the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act establish data security requirements for personal health information;
- the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA) define data security requirements for personal credit card information and credit report information; and
- the United States Federal Trade Commission (FTC) determines whether companies whose data security has been breached have engaged in unfair or deceptive trade practices.

At the state level, nearly every state has enacted data security or security breach notification laws that potentially have nationwide applicability for companies, regardless of where they are located, that have collected personal information of citizens of those states. Data security requirements in some states, such as Massachusetts, Nevada and Oregon, are quite specific and detailed.

Due diligence that a company is legally required to undertake before disclosing personally identifiable information to a service provider typically includes inquiry about whether the service provider has an information security program, whether the information security program appropriately addresses known and anticipated hazards and threats to data security, and whether the service provider has implemented and adheres to its information security program. Fulfilling this due diligence obligation can require significant effort and resources, and companies that have a need to make personal information available to third-party service providers may not be properly prepared or equipped to meet the obligation. Nevertheless, failure to fulfill this obligation exposes a company to liability.

Independent certification of compliance with the International Organization of Standardization (ISO) and International Electrotechnical Commission (IEC) 27001 standard, commonly known as ISO 27001, is sound evidence that a service provider has implemented and adheres to a reasonable information security management system with appropriate policies, controls, processes and procedures. ISO 27001 requires ten categories of assessment of an information security management system: information security policy, security organization, personnel security, access controls, physical security, asset classification controls, continuity planning, system deployment, communication management, and compliance. ISO 27001 certification represents an independent auditor's conclusion that:

- the certified company has developed an "information security management system" (i.e., an information security program) with technical, physical and administrative safeguards to protect the confidentiality, integrity, and availability of personal information and other confidential data; and
- the certified company and its employees, through training and other measures that the auditor has examined, are cognizant of data security issues and are addressing them on an ongoing basis.

The effort and expense that a company must invest to obtain and maintain ISO 27001 certification demonstrate that the certified company takes data security seriously.

Chenxi Wang, Principal Analyst at Forrester Research, Inc., has stated that "[ISO 27001] is the best [information security] standard there is."¹ An article in *IT World*, which is published by International Data Group, concludes that "ISO 27001 plays a very important role in monitoring, review, maintenance and improvement of [a company's] information security management system and will likely give other organizations and customers greater confidence in all the ways they interact with [the company]."²

Data obtained from ISO in November 2010 for the period from 2006, when ISO 27001 certifications began, through 2009, the latest period for which data is available, shows that a total of only 35,709 certifications worldwide were granted during the period.³ The total number of certifications granted in 2009 was only 12,934.⁴ Of the companies in 2009 reporting certification data by industry segment, only approximately 148 certifications were obtained worldwide in the industry segment relevant to the insurance industry and approximately 102 were obtained worldwide in the health industry segment.⁵ When viewed in context of the millions of companies that exist worldwide, a large number of which likely collect personal information, the data demonstrates that a very small number of companies have been determined by independent auditors to satisfy the ten categories of ISO 27001 standards.

Companies that make confidential information available to a third-party service provider should carefully consider the contribution that ISO 27001 certification can make not only to fulfillment of their due

¹ "Microsoft Wants ISO Security Certification for its Cloud Services", Computerworld, Oct. 23, 2009, available at http://www.computerworld.com/s/article/print/9139820/Microsoft_wants_ISO_certification_for_its_cloud_services.

² What Does ISO 27001 Mean to You, *IT World*, Feb. 24, 2010, available at <http://www.itworld.com/security/97767/what-does-iso-27001-mean-you>

³ The ISO Survey of Certifications, 2009, available at <http://www.iso.org/iso/pressrelease.htm?refid=Ref1363> for a fee. The survey comprises data collected by Nielsen Company, Austria, and analyzed by the ISO Central Secretariat.

⁴ *Id.*

⁵ *Id.* Because not every entity responded with sector specific information, the data is a general indicator of the sector information. In the industry segment relevant to the insurance industry where data was reported, that segment constituted less than 4% of reported certifications and the health care data constituted less than 3% of reported certifications.

diligence obligations under federal, state and local laws and regulations but also to the security of their sensitive business information. A careful examination of the steps a service provider takes to protect the privacy and security of its clients' confidential information could be critical to avoiding unauthorized disclosure of competitively sensitive information to competitors as well as avoiding liability for any data security breach or that occurs despite the fact that the company has itself been vigilant about protecting its confidential information.