



# Data Protection Legislation

**recall**<sup>TM</sup>  
Your Information. Securely Managed.

## Data Protection Legislation

The ability to trace, track and find critical data is essential when complying with regulatory requirements such as:

### Gramm-Leach-Bliley Act (GLBA), 1999

GLBA requires financial institutions to provide administrative, technical and physical tools to protect the integrity and confidentiality of their customer records. Companies must also ensure the availability of financial information and business continuity. Failure to comply can result in fines of up to US \$1 million in addition to other penalties.

### Sarbanes-Oxley Act (SOX), 2002

SOX was enacted as a direct response to corporate scandals of companies such as Enron and WorldCom. Its regulations ensure the integrity of corporate financial information and deal with corporate governance. SOX affects US publicly traded companies but can globally impact their officers, boards and auditors, holding them personally accountable for the accuracy and maintenance of financial information. Significant penalties and fines - including jail terms - can apply.

### Health Insurance Portability and Accountability Act (HIPAA), 1996

HIPAA was enacted to protect health insurance coverage for workers and their families when they change or lose their jobs. One section, Title II, requires the creation of standards for electronic patient health records, administrative and financial data, and the protection and security of health-related data. HIPAA can affect any organization involved or related to healthcare. It can even extend to companies that are providing services to the healthcare sector such as information system providers. Even though HIPAA does not specify measures on compliance, failure to reasonably protect information covered by HIPAA can result in fines of up to US \$250,000 and up to 10 years of imprisonment.

Ongoing or scheduled audits are required to confirm the accuracy and availability of the information specific to the aforementioned acts. Systems are often tested to ensure they deliver the relevant information in a timely manner. Also, the length of retention can be up to 7 years for the financial data and for the health sector, while the data handled by the health sector may need to be retained for over 20 years. The key point is that this information must be readily available at any time and that its content can span a considerable time period.

In Australia, Privacy Act, 2001, under Principle 4, Storage and Security of Personal Information, requires the “keeper” of records to ensure that the information contained in them is protected against loss, unauthorized access and use, modification, disclosure, and any other form of misuse by taking security measures that are reasonable and within the record keeper’s power to use. Non-compliance will leave the keeper of the records personally liable and subject to prosecution.

Nearly every country in which Recall operates has now introduced some form of legislation to ensure that sensitive information is protected. Usually it is financially based and initiated by the Monetary or Financial Service Authority of the country. For the European Union refer to the Markets in Financial Instruments Directive (MiFID) and for the UK, the Data Protection and Freedom of Information Acts.

\* Source: B&L Associates, “Compliance through Proper Tape Management