



## Frequently Asked Questions: Regulatory Compliance

### What regulations am I likely to encounter?

State and federal regulations often set rigorous standards for data protection and privacy. Depending on your industry, your IT infrastructure will need to meet these requirements, and ezTechDirect can help. Most often, regulations govern industries and the way information is kept and transmitted. Some industry-specific regulations include:

- Sarbanes-Oxley (SOX) Section 404 for Accountants
- PCI DDS Requirements 3, 4, 7, and 9 for Retailers
- Gramm-Leach-Bliley Section 501 (b) for Bankers
- HIPAA's Security Rules for Medical and Dental Offices
- State Legislation like MA 201 CMR 17 and similar laws

### How do these regulations impact data security, storage, backup and recovery?

While these laws govern different industries, all address three common, key items:

- Protection of data from loss/destruction
- Encryption of data over open networks
- Limited physical access to stored data

Regulations prescribe standards for how information is stored, secured, archived and accessed. In some cases, companies are required to maintain records for a period of years and ensure they're well safeguarded. Working with ezTechDirect, you can create the IT infrastructure you need to support relevant compliances. ezTechDirect Backup and Recovery can be a key part of your overall solution, as it offers a highly secure backup supported by redundant data centers that meets or exceeds regulations regarding protection, encryption and physical access.



### **What's my risk if we're not compliant with industry regulations?**

If you fail to comply with relevant regulations, you could face heavy fines and penalties. The U.S. Department of Health and Human Services is responsible for HIPAA-compliance enforcement. Credit card providers will fine retailers who don't follow PCI guidelines. The SEC oversees Sarbanes-Oxley, which can carry criminal penalties for violations.

Penalties can be substantial. Several multi-million dollar fines have been issued against healthcare providers and insurers found in violation of HIPAA guidelines. In 2012, the agency started turning its attention to smaller providers; a five-physician practice based in Phoenix was fined \$100,000 in 2012 following an investigation that found the practice failed to safeguard patient information and take other security measures. PCI violations can often carry five-figure penalties against small, independent retailers who don't safeguard consumer credit card data. In short, the risk is substantial and real.

Beyond fines and punitive action, you can face the risk of lawsuit liabilities and the damaging impact to reputation and lost business that negative publicity would inevitably bring.

### **Will I be compliant if I use ezTechDirect Backup and Recovery?**

ezTechDirect is a cloud backup, archiving and recovery solution that automates the processes of securely backing up electronic data and file recovery. It was created with these data protection regulations in mind to satisfy the broad need for a safe, reliable, and cost-effective method of backing up data offsite and allowing full file restoration at any time from any authorized location. ezTechDirect provides a highly secure solution that can be used to meet or exceed regulatory compliance when scheduling, encryption, and archiving rules align with regulations.