UNTANGLE THE COMPLIANCE WEB

Understanding the federal and state compliance regulations can help agencies determine which ones apply.

Depending on the mission, scope, location and type of data collected, state and local agencies must comply with a possibly confusing array of both data privacy laws and industry-specific regulations. Determining which regulations apply isn't always easy. Here are some of the most common, along with guidelines for when they may apply:

FEDERAL REGULATIONS:

FISMA (Federal Information Security Management Act): State agencies administering federal programs such as Medicare, for example, must meet this standard. FISMA defines a framework for protecting government information, assets, and operations.

FedRAMP: (Federal Risk and Authorization Management Program): Many states require agencies using cloud services to insist on FedRAMP certification, and it's encouraged by the GSA. FedRAMP is a government-wide program providing a standardized approach to assessing cloud security.

NIST SP 800-53: This requires organizations to maintain specific security and privacy controls on federal information systems. Many states now require compliance with 800-53 as a security baseline.

NIST SP 800-171: This standard for controlled unclassified information (CUI) is required for state and local agencies, as well as universities and others handling federal data.

FIPS 140-2: This specifies the security requirements for cryptographic-based security systems. Compliance is mandatory for state and local government agencies where projects are spending federal money.

HIPAA: This is required for any organization handling personal healthcare information.

CJIS (Criminal Justice Information Service): This outlines security standards for all criminal justice organizations in the United States.

Other federal oversight protections help safeguard employee and citizen information, including:

- **American with Disabilities Act:** this pertains to employee disability information
- **Family and Medical Leave Act:** this pertains to medical leave information
- **Fair Credit Reporting Act):** this pertains to credit history, criminal history checks, and so on.

Industry data privacy and security standards are also frequently relevant to state and local agencies. The most pervasive is PCI-DSS (Payment Card Industry Data Security Stan dard), which requires privacy protection of payment card data.

STATE AND LOCAL REGULATIONS:

These vary by state and municipality, so it's important to check local jurisdictions. Some examples include:

- New York's requirements for retention and destruction of records
- California's data breach notification law, now being adopted by many other states
- Restricted government access of online communications, currently in use by California and Connecticut, and under consideration by New Mexico
- Data disposal laws requiring agencies to destroy or dispose of personal information so it's unreadable. More than half of states currently have such laws in place.

Get Ready for GDPR

If you haven't heard much about GDPR, you will soon. The General Data Protection Regulation, which goes into effect on May 25th, is designed to protect the data privacy rates of citizens and residents of the European Union. While that may not seem important for state and local agencies, it definitely will affect them. It applies to any organization handling health records, addresses or any other data of European residents, even if those organizations are based in other countries. That means it will affect not only U.S.-based companies, but public sector organizations as well.

"A public sector organization that holds data on an American citizen who moves to the EU, an EU resident who lived in the United States and then moved back to Europe, or even a visitor from the E.U. is accountable," explains Michael Osterman, president of Osterman Research, a Black Diamond, Wash., consultancy that has studied the issue. "All of that data would be subject to GDPR compliance. There is no exception for public sector organizations in the GDPR, and Articles 4 and 37 specifically call out the public sector as being subject to compliance."

Noncompliant organizations can be fined. For commercial organizations, that fine can reach $20 million, but the fine for public sector organizations is unclear. While GDPR compliance may be complex and expensive, Osterman says it's actually a good thing. It not only forces organizations to understand where all data is located and how it should be classified based on the sensitivity of the information it contains, but it forces agencies to implement appropriate safeguards for data management, including encrypting data at rest and in transit, DLP solutions to monitor sensitive data sent unencrypted, and other security solutions.