Organizing a Privacy Program:
Administrative Infrastructure and Reporting Relationships

Presented by: Samuel P. Jenkins, Director
Defense Privacy Office

Former Privacy Officer, DoD Tricare Management Activity

AGENDA

Opening Thoughts

Organizational Assessment

Privacy Program Development

Ongoing Activities

Monitoring and Reporting

Opening Thoughts

The health care industry uses one of the largest networked information systems in the country. The information technology and many interfaces required to meet the needs of the healthcare industry continue to expand.

With this expansion we are also experiencing a similar increase in privacy incidents (loss, theft or compromise) and breaches of information (identity theft, healthcare fraud, malicious intent).

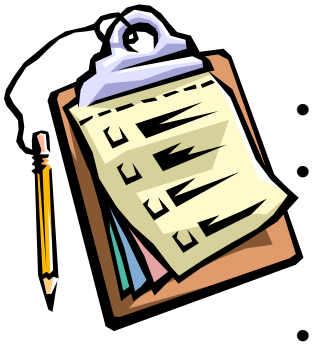
The Nations concern for personal privacy is not new particularly in health care. Becoming privacy compliant is a process first through an assessment of where we are and a determination where we desire to be followed by a plan to get and stay there.

The application of privacy standards for personally identifiable information and protected health information has evolved over time. Organizations must continue to grow in order to stay ahead of these changes.

The standards that are most important are those that matter the most to the customer.

Organizational Assessment

Determine where the organization is in relation to its privacy requirements –



- Identify information systems and processes
- Document all locations of personal information (files, databases, paper copies, CDs, hard drives, tapes and any other storage medium)
- Map the processes associated with the above locations against the requirements of the organization the collect, use, share, process, maintain, store and destroy information
- Compare current policies against the requirements of applicable privacy legislation or regulation to establish a gap analysis between existing and required standards
- Identify risks associated with data, uses and compliance to create a strategic plan and working document to achieve compliance

Privacy Program Development
(Refreshment)

Establish infrastructure

Position descriptions

- Chief Privacy Official
- Privacy team leads
- Key Privacy personnel

Compliance reporting lines

- Policy and compliance monitoring
- Training and refresher training completion and documentation
- Incident reporting and follow-up

Designate authority over privacy issues

- Develop teams and identify key personnel for privacy actions related to documents, systems, information sharing, transfer, storage and others
- Empower employees throughout the organization

Ongoing Activities

Development and implementing policies, procedures training and making changes as required –

- Change forms, systems, procedures and manuals to reflect privacy requirements
- Change or develop systems to address and support privacy compliance. Network coordination of policy development and implementation throughout the organization
- Review holdings and archived information for protections (both privacy and security requirements)
- Train, refresh, retrain. Learning is not just acquiring more information but instead it is about expanding the results we truly want.
- Create anonymous lessons learned from incidents to educate staff on issues and ways to avoid them

Monitor and Report for Compliance

To ensure you get to the desired compliance

- Re-assess results with policies to measure outcomes and show due diligence toward compliance
- Determine criteria for measurement of training completion, incident reporting and management actions
- Create an environment that encourages the reporting of incidents
- Identify thresholds for escalating issues to senior management
- Establish a means of communication for staff, patients and other persons with inquiries, concerns or issues

Ensures that appropriate reporting procedures are developed and implemented and that there is a mechanism for follow-up, communication, re-training and resolution of issues.

Ensures that appropriate reviews and audits are conducted to provide assurance that privacy policies, procedures and technology create a compliant environment.

Conclusion

A privacy compliant organizational structure allows adoption of methodologies in addressing the privacy issue it faces.

The organization can address in a systematic and planned way, specific privacy requirements, including personal information policies, procedures and standards.

An adequate privacy compliance program can create or improve consumer trust and improve the protection of information for consumers and employees alike.

Publicity of privacy violations can cause damage to an organizations reputation and possibly its ability to attract patients.

Defense Privacy Office

Samuel P. Jenkins, Director

1901 S. Bell Street, Suite 920

Arlington, VA. 22202

(Email) DPO.Correspondence@osd.mil

(Office) (703) 607-2943

(Fax) (703) 607-2951

Defense Privacy Office