AASP BEST PRACTICES

ADVANCEMENT TECHNOLOGY

Title: Best Practice in Data Security

Original date:	April 14, 2014
Revision date:	July 13, 2021 (previously revised March 25, 2016)
Originally prepared by:	Lynne Becker with Terry Callaghan and Amy Marks
Revised by:	Vidya Kagan and David Woodley
Category:	Advancement Technology
Comments to:	bestpractices@advserv.org (please include the name of the Best Practice in the subject line)
Comment Period:	June 2021 - July 2021

Description of Practice:

All organizations should develop an organizational data security strategy to protect critical information. Data security is not only a great idea to protect your constituents' data, it's probably also required by one governing body or another depending on your industry. It's recommended that data administrators familiarize themselves with federal and state laws and regulations that govern data protection. For instance, education records are protected by FERPA (Family Education Rights and Privacy Act) or HIPAA. Each state also has its own laws and regulations for handling confidential data. Lastly, your institution probably has policies and procedures that your advancement policies will need to be consistent with. Penalties exist at all levels and can add up quickly. It becomes worse if exposed constituent data results in lawsuits against the institution. Hence, data security should be a major consideration.

Prospective Users of Practice:
Advancement professionals, information management colleagues, IT colleagues, data professionals.

Issues Addressed:
PHI, PII, encryption software, state laws.

Desired Outcome:
We will provide an outline of things to consider when creating a data security policy for your organization.

AASP Recommendation:

Protecting Data in a system (data at rest)
Organizations should have the answers to these questions:

- **Where is your data?** Organizations should know what data they have and where their data is stored, e.g. is it stored across multiple devices, in the cloud, on-site, etc.
- **Who accesses your data?** Organizations need to understand who is accessing what data, how it is being used, and where it is going. Data needs to be categorized according to sensitivity and accessibility. The more people who have access to data, the higher the chances that data security will be an issue.

Protecting Data as it is networked (data in transit)

IT takes the lead on this area, but there are a few things advancement departments should be aware of:
-use of secure, protected networks
-use of VPNs
-avoiding potentially unsafe networks
-ensuring use of firewalls

Protecting Data as it is shared or leaves a data system and network

Organizations should create policies about controlling data transfers from all desktops and laptops. For example, data could be copied from the network onto USB drives, MP3 players, CDs, DVDs, and other removable media and fall into the wrong hands. Here are some items that advancement and technology professionals should consider:
-use of temporary sharing arrangements (time limited access supported by Google Drive, etc.)
-use of encrypted passwords for documents

Methods to ensure data security

Use of encryption software:
From an article published by Norton Security: “Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information.” Encrypting data is important for three main reasons: data privacy, protection from hackers, and regulatory compliance.

Encryption software can help to protect the data an organization sends, receives, and stores. There are several types of encryption: DES, Triple DES, RSA, AES, TwoFish, and encryption via SSL. It is important for organizations to:

- Install and use trusted security software on all devices
- Keep your security software up to date
- Update your operating system and other software on a regular basis
- Back up your data regularly
- Consider utilizing cloud services

Cloud security:
Cloud computing is defined as “the delivery of hosted services, including software, hardware, and storage, over the Internet.” There are many benefits to cloud computing, including rapid deployment, flexibility, minor up-front costs, and scalability. Cloud computing is virtually universal among organizations of all sizes.

Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats. Cloud security responsibility is typically shared between the cloud provider and the customer. There are three categories of responsibilities: responsibilities that are always the provider’s, responsibilities that are always the customer’s, and responsibilities that vary depending on the service model.

The public cloud does not have clear perimeters and is thus a fundamentally different security reality. Organizations should be aware of how they use the cloud, the strengths of their cloud provider, and the security challenges inherent in this set-up. Some cloud providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform offer native security features and services. Organizations may decide to contract with third-party cloud security providers to achieve additional protection against breaches, data leaks, and cyberattacks. Before committing to contracts, organizations should review vendors' privacy policies, security environments, and data breach response and mitigation plans.

PII and PHI

It is important to understand that personal information is classified in several different ways. Common terminology includes Personal Identifiable Information (PII) and Protected Health Information (PHI).

Personal Identifiable Information (PII)

According to the Department of Labor website, PII is defined as "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media. …The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information."

Protected Health Information (PHI)

The U.S. Department of Health & Human Services website states that "PHI stands for Protected Health Information. The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes."

Furthermore, according to industry publications,"Protected health information is the term given to health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services. Protected health information is often shortened to PHI, or in the case of electronic health information, ePHI.

The HIPAA Security Rule requires safeguards to be implemented by HIPAA-covered entities and their business associates to protect PHI that is created, used, received, stored, or transmitted in electronic format. Administrative, physical, and technical controls must be implemented to ensure the confidentiality, integrity, and availability of ePHI. Failures to protect ePHI and subsequent privacy violations can result in significant fines, although since there is no private cause of action in HIPAA, patients affected by data breaches cannot sue HIPAA covered entities for the exposure, theft, or impermissible disclosure of their PHI.

The HIPAA Privacy Rules stipulates allowable uses and disclosures of PHI and gives patients the right to obtain a copy of the PHI that is held by their healthcare providers. HealthIT can be used to help patients access their PHI. Many healthcare providers now allow patients to access some or all of their health information via patient portals. If only partial information is available through a patient portal, patients can still exercise their right to obtain all PHI in a designated record set held by their healthcare providers by submitting a request in writing.”

State laws

Each state may have its own guidelines around data security. For example, California has adopted the California Consumer Privacy Act (CCPA) of 2018, which defines “penalties for companies that expose consumer data due to a breach or security lapse. It also allows courts to offer “injunctive or declaratory relief,” or “any other relief the court deems proper.”” Businesses are not required to report breaches under AB 375, and consumers must file complaints before fines are possible. The best course of action for security, then, is to know what data AB 375 defines as private data and take steps to secure it. Again, any organization that complies with the GDPR likely does not need to take further action to comply with AB 375 in terms of securing data.

Creation of a Formal Written Policy, End User Adoption, Training

Once the organization has the information outlined above, then they can create effective and accurate policies to protect the data. Policies should be expansive and cover all situations, yet flexible enough to accommodate new issues and business practices. From McAfee: “Enforcing the right policies at the right time is essential to ensuring data security, regulatory compliance, and intellectual property protection.”

Data Security Policy

The AASP Best Practices group strongly recommends creating a formal written policy for how security and data privacy will be addressed. The policy should include at a minimum:

How does the institution *value* constituent data?

What entities within the organization bear responsibility for securing data?

What entities will be accessing data and for what reasons?

With whom will data be shared?

How will data be updated?

What data is considered confidential and what is considered sensitive?

What is the risk mitigation strategy (what tools will it employ to keep data secure)?

How can constituents opt out of having their data shared or maintained?

How is data secured in transit, while it is being moved across the network?

How is data secured as it is physically handed off from one person to another either in an electronic or paper format?

How is data secured in the cloud?

What are the federal and state data security laws that apply to your organization?

Resources/Bibliography:

https://www.mcafee.com/enterprise/en-us/security-awareness/data-protection/data-security-best-practices.html

https://us.norton.com/internetsecurity-privacy-what-is-encryption.html

https://www.spirion.com/solutions/compliance/

https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html

Department of Labor website (https://www.dol.gov/general/ppii)

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

https://www.hhs.gov/

https://www.hipaajournal.com/what-is-protected-health-information/

California Consumer Privacy Act (CCPA) of 2018: https://oag.ca.gov/privacy/ccpa

https://www.csoonline.com/article/3526495/the-ccpa-is-an-opportunity-to-get-your-data-security-house-in-order.html

https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/