Security standards

PCI-DSS, HIPAA, FISMA, ISO 27001

End Point Corporation, Jon Jensen, 2014-07-11

PCI DSS

Payment Card Industry Data Security Standard

There are other PCI standards beside DSS but this is the one that applies to any company taking or processing credit card information or developing or hosting software that does.

Merging 5 standards into one

PCI was founded by Visa, MasterCard, American Express, JCB, and Discover.

Before joining forces, they each had their own security standards.

Who’s Who: Banks

Visa and MasterCard are made up of Member organisations who can be either Acquirers or Issuers (or both).

Acquirers handle Merchants.

Issuers issue the cards to Cardholders.

Who's Who: The Rest of Us

Merchants: those entities who accept card transactions.

Cardholders: those trying to spend their money.

Service Providers: those providing any service requiring the processing, storing or transport of card information on behalf of any of the above.

How PCI DSS is applied

Externally: by regular remote Network Security Scan by an approved vendor.

Internally: Self Assessment Questionnaires ask about compliance with each of the standard’s requirements.

Onsite: Very large merchants must have an annual onsite review and audit.

PCI DSS teeth

Penalties can be passed on to Merchants and Service Providers through their contracts, including monetary charges and account cancellation (kiss of death to ecommerce providers).

PCI DSS Merchant Levels

There are several Merchant Levels. In the past small merchants doing fewer than a certain number of transactions per year had less of a compliance burden.

Now, the only difference is that very large merchants must have an annual onsite audit. For us, Merchant Levels don’t matter.

Are we a Service Provider?

No. We do not offer payment processing services to third parties on our own infrastructure.

We offer development and hosting services for our clients, and some of them are Merchants. (None of them are Service Providers to third parties either.)

Network Security Scanning

Typically automated and run daily.

Targets Internet-facing:

- routers and firewalls
- servers and hosts
- applications

Scan reporting

Scans report to the Merchant about issues found, categorizing on severity scale of 1 to 5:

- 1: informational
- 2: recommended changes
- 3: high, limited remote exploit causing risk
- 4: critical, potential remote data exposure
- 5: urgent, serious remote exploits

Scan remediation

Severity levels 3-5 must be dealt with immediately, and confirmed solved by another scan.

Merchants can have their accounts frozen or contracts canceled if they don’t comply.

Self Assessment Questionnaire

Don’t expect to be quick. Is fairly large and has many, many questions that are not quick to find answers for.

Mainly includes Yes/No/Not Applicable choices.

Our clients are responsible. We can only help by answering some for them; many involve office network, host, and physical security, etc.

PCI DSS requirements

Review the requirements documents yourself when you’re helping a client. Good to know specifics.

PCI DSS reqs. in broad strokes

- No default passwords
- Disable unused services
- Secure wireless networks
- Regularly apply software updates
- Use firewalls
- Use anti-virus software where available
- Unique account for each user

PCI DSS reqs. in broad strokes

- Log all access attemps
- Audit logs
- Require minimum password strength
- Configure crypto well, e.g. https
- Train periodically
- Must document flow of cardholder data

Cardholder Data

Can store:

- Primary Account Number (PAN), but must be encrypted or masked to first 6 + last 4 digits
- Cardholder name
- Service code (number on the magnetic stripe that specifies the acceptance requirements and limitations for magnetic stripe read transactions)
- Expiration date

Sensitive Authentication Data

Cannot store, not even encrypted or masked:

- Full Track Data (magnetic stripe)
- Card security code (CAV2/CVC2/CVV2/CID)
- PIN/PIN block

Crypographic key custodians

Don’t store cardholder data unless absolutely necessary, even in encrypted form.

(3.5) Keys must be rotated regularly (e.g. every few years). Must designate “key custodians”. Restrict access to keys to the fewest number of custodians necessary. Key custodians must sign a formal agreement of understanding.

Data Retention and Disposal Policies

Limit data storage to what is necessary

… for as long as necessary.

Document reasons for “necessary”.

Securely delete data when no longer needed.

Quarterly review systems to ensure nothing is being stored beyond what is specified.

PAN encryption + masking risk

(3.4) “It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity’s environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.”

Code Reviews Required

(6.3.2) Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices.

Code-review results are reviewed and approved by management prior to release.

HIPAA

Health Insurance Portability and Accountability

Medical data

Covers printed, spoken, and electronic forms.

CDC incorporates HIPAA security standards.

3 types of security safeguards

- administrative
- physical
- technical

Access events

- authorization
- establishment
- modification
- termination

PHI, EPHI

Protected health information. Electronic PHI.

Any information that can be used to identify a patient – whether living or deceased – that relates to the patient's past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.

Personal Identifiers

- Patient names
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses

More Personal Identifiers

- Geographic subdivisions (smaller than state), including zip code!
- Dates, unless only the year is present!

Even more Personal Identifiers

- Names of relatives
- Full face photographs or images
- Healthcare record numbers
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Certificate/license numbers
- Any other unique number, code, or characteristic that can be linked to an individual.

HIPAA Enforcement Rule

HHS issued the Final Rule regarding HIPAA enforcement and it took effect on March 16, 2006. The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violation.

HIPAA Security Breach Fine

A fine of $50,000 to the Hospice of North Idaho (HONI) was made for a potential HIPAA Security Rule breach affecting fewer than 500 people. Rachel Seeger, a spokeswoman for HHS, stated, “HONI did not conduct an accurate and thorough risk analysis to the confidentiality of ePHI as part of its security management process from 2005 through Jan. 17, 2012.” This investigation was initiated with the theft from an employee’s vehicle of an unencrypted laptop containing 441 patient records.

Breach Reporting

Part of all security standards is reporting. Even just suspicions. Longstanding bad practices. Immediately.

We keep a timestamped trail for reporting.

Breach reporting to ...

Simplified: I am End Point's Chief Privacy Officer, Chief Security Officer, and the equivalent responsible party for security in any of these standards. Report to me as a top priority. If you can't reach me right away, report to directors@endpoint.com and security@endpoint.com.

Reporting timeliness matters

How quickly and responsibly we respond to breaches makes a huge difference in how the breach will be viewed and the consequences of it.

Public reporting

See:

https://www.endpoint.com/contact

We offer a PGP public key and a reporting address that will go to the hosting team and anyone else who needs to know.

FISMA

Federal Information Security Management Act of 2002

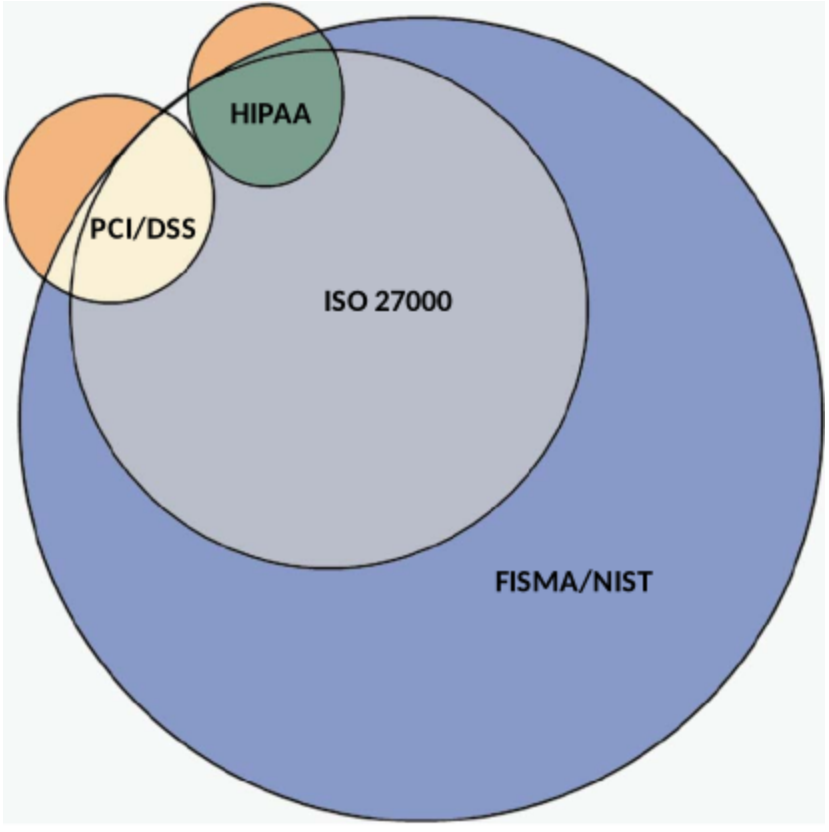
Applies to federal agencies and their contractors.

ISO/IEC 27001:2013

A specification for an information security management system.

An international equivalent of some of the U.S. standards.

Compliance compatibility



Security Provisions Overlap/Comparison

Ongoing

It’s a process, not a destination.

Reference

- https://www.pcisecuritystandards.org/
- http://www.hhs.gov/ocr/privacy/
- http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002
- http://en.wikipedia.org/wiki/ISO/IEC_27001:2013
- http://www.catapulttechnology.com/pdf/Insights_Files/white_papers/Information_Security_White_Paper.pdf