DICKINSON WRIGHT PLLC

presents

REMOVING THE "CRYPTIC" FROM ENCRYPTION: HIPAA AND THE MEANING OF SECURE PHI

Brian R. Balow, Member

OnlineTech Webinar

September 17, 2013

Overview

❑ HIPAA Administrative Simplification Regulation (the Stick)

❑ CMS and Meaningful Use (the Carrot and the Stick)

❑ HIPAA breaches can result in large fines and bad publicity

❑ Achieving Meaningful Use results in payments, and failure to achieve MU results in reduced reimbursement

❑ Encrypting PHI can lessen HIPAA exposure and assist in achieving Meaningful Use

Overview

- ❑ What (requires protection)?
- ❑ Why (is protection important)?
- ❑ How (should it be protected)?
- ❑ Who (should encrypt)?

Overview

- □ A word about our Sponsor: There are excellent existing materials available on the Online Tech website regarding other (and related) aspects of encryption:

http://resource.onlinetech.com/hipaa-security-checklist-for-healthcare-organizations/

http://www.onlinetech.com/events/encryption-perspective-on-privacy-security-a-compliance

http://resource.onlinetech.com/encrypting-data-to-meet-hipaa-compliance/

WHAT?

❑ "Protected Health Information" means individually identifiable health information

❑ '"Individually Identifiable Health Information" means information that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and [t]hat identifies the individual; or [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.'

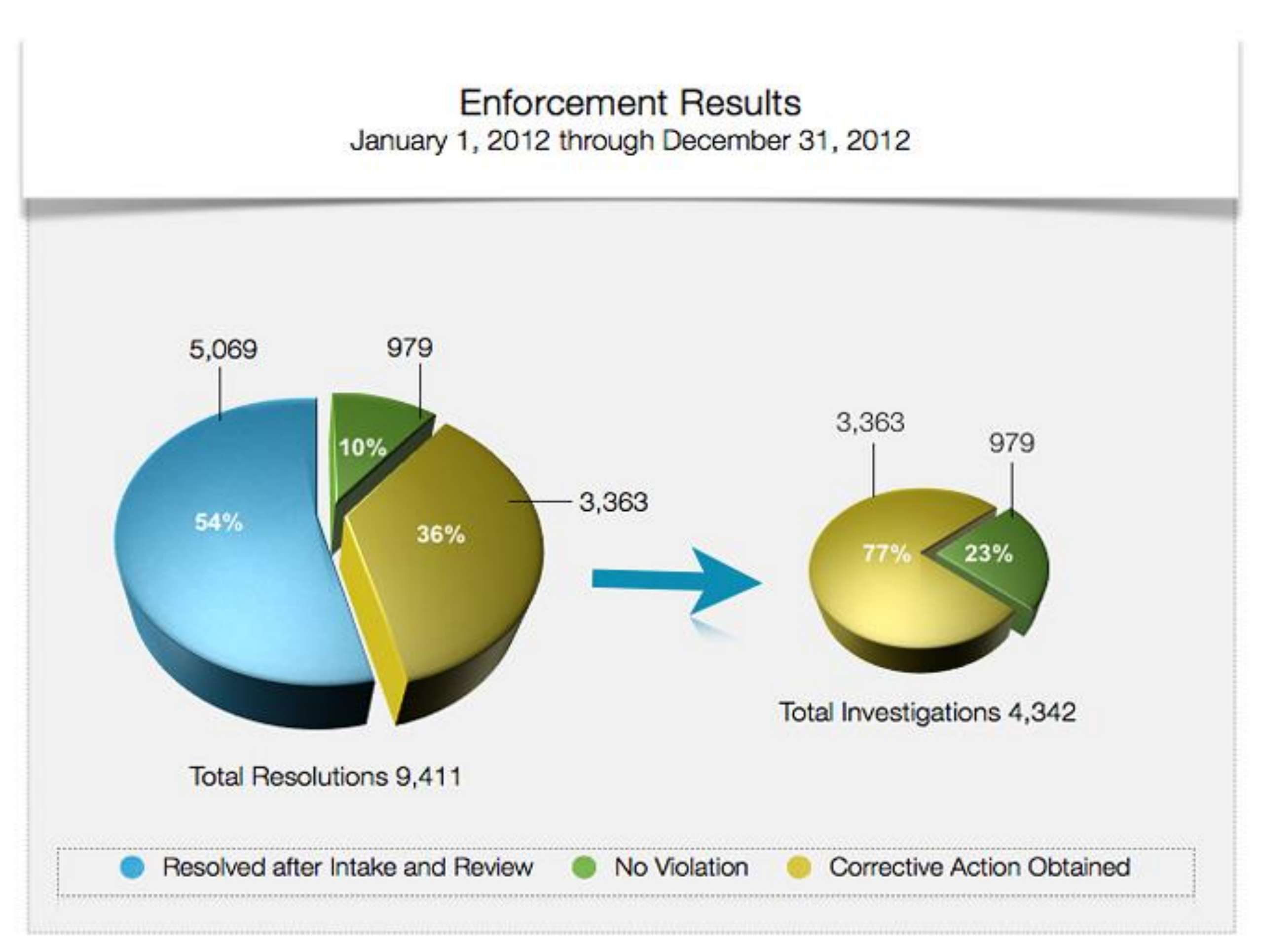
❑ Much overlap with other "PII"-centered laws, regulations, and industry standards (e.g., state data breach notification laws; PCI Data Security Standard; GLBA)

WHY?

- ❑ **Enforcement Rule**: Sets the liability standards and the penalties for noncompliance with the Privacy Rule and the Security Rule

- ❑ **Breach Notification Rule**: Sets the parameters under which a covered entity must provide notice of an "acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information."

OCR Enforcement of Data Breaches



Enforcement Results

January 1, 2012 through December 31, 2012

HIPAA Civil Money Penalties

VIOLATION TYPE	EACH VIOLATION	REPEAT VIOLATIONS/YR
Did Not Know	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

WHY?

- ❑ *The Security Rule*: *Encryption and decryption* ***(Addressable)***. Implement a mechanism to encrypt and decrypt electronic protected health information. 45 CFR §164.312.

- ❑ "Addressable": The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework. For example, a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative. This decision will depend on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.

WHY?

- □ *The Breach Notification Rule*: (a) *Standard* —(1) *General rule*. A covered entity shall, following the discovery of a breach of **unsecured protected health information**, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. 45 CFR §164.404.

WHY?

Meaningful Use, Stage 2 (45 CFR §170.314(d)(7)):

(7) *End-user device encryption.* Paragraph (d)(7)(i) **or** (ii) of this section must be met to satisfy this certification criterion.

(i) EHR technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of EHR technology on those devices stops.

(A) **Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(1).**

(B) *Default setting.* EHR technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(ii) EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR technology on those devices stops.

Meaningful Use Incentives/Penalties

❑ To receive the maximum EHR incentive payment, Medicare eligible professionals must begin participation by 2012.

❑ Eligible professionals who demonstrate meaningful use of certified EHR technology can receive up to $44,000 over 5 continuous years under the Medicare

❑ Incentive payments for eligible hospitals: http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/MLN_TipSheet_MedicareHospitals.pdf

❑ Beginning in 2015, Medicare eligible professionals who do not successfully demonstrate meaningful use will be subject to a payment adjustment. The payment reduction starts at 1% and increases each year that a Medicare eligible professional does not demonstrate meaningful use, to a maximum of 5%.

HOW?

- ❑ HIPAA: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached.
- ❑ To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.

HOW?

- ❑ HIPAA:

The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) **and judged to meet this standard**.

(i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

(ii) Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

How?

http://resource.onlinetech.com/encrypting-data-to-meet-hipaa-compliance

HOW?

❑ **CMS Meaningful Use**: "We did not propose to change the HIPAA Security Rule requirements, or require any more than is required under HIPAA. We only emphasize the importance of an EP or hospital including in its security risk analysis an assessment of the reasonable and appropriateness of encrypting electronic protected health information as a means of securing it, **and where it is not reasonable and appropriate, the adoption of an equivalent alternative measure**."

❑ 45 CFR §170.210(a)(1): Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2

❑ Test Procedure: http://www.healthit.gov/sites/default/files/170.314d7_enduserdeviceencryption_2014_tp_approvedv1.2.pdf

WHO?

❑ Encryption is one of many tools, and is not required in all environments

❑ IF you are an EP, EH, or CAH, the likelihood is that encryption makes sense (to achieve Meaningful Use)

❑ IF you are not one of the above, but are a covered entity or a business associate, your risk assessment (required under the Security Rule) should guide your decision on whether to encrypt

WHO?

❑ Breach Notification Rule alone, may be enough to drive an decision to encrypt (due to potential negative publicity if reporting is require)

❑ Like most regulatory and legal considerations, one size does not fit all, and context matters.

Breach Notification Rule, Cont'd

❑ Risk Assessment:

1. Nature and extent of PHI involved (including identifiers/likelihood of re-identification)
2. Consider the recipient (e.g., already under HIPAA obligation?)
3. Was PHI actually acquired or viewed
4. Extent to which risk has been mitigated

Disclaimer

This presentation is informational only. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation

ONLINE TECH

Upcoming Events:

September 21 – Two-Day Essential Vmware Boot Camp

September 23-24 – HIMSS Privacy & Security Forum

October 16-17 – Detroit SecureWorld 2013

Contact Us:

Email - contactus@onlinetech.com

Phone - 877.740.5028

Web - www.onlinetech.com

White Papers - www.onlinetech.com/resources/white-papers

Contact Information

Brian R. Balow

248-433-7536

bbalow@dickinsonwright.com

Thank you for your time and attention