United States Department of Health & Human Services
Office of the Secretary
Office for Civil Rights (OCR)

HIPAA/HITECH Omnibus Final Rule

April 12, 2013

HHS Office for Civil Rights

Omnibus Components

- Final Rule on HITECH Privacy, Security, & Enforcement Provisions (and certain non-HITECH changes) (proposed rule published July 2010)
- Final Rule on new HITECH CMP Structure (interim final rule published Oct. 2009)
- Final Rule on HITECH Breach Notification (interim final rule published Aug. 2009)
- Final Rule on GINA Privacy Provisions (proposed rule published Oct. 2009)

Not in Omnibus

- HITECH Accounting of Disclosures Rule
- HITECH Distribution of Penalties/Settlements to Harmed Individuals Rule
- HITECH Minimum Necessary Guidance
- HIPAA/CLIA Patient Access to Laboratory Test Reports Rule

Important Dates

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Transition Period to Conform BA Contracts – Up to September 22, 2014, for Qualifying Contracts

Outline of Topics

- HITECH Privacy & Security
  - Business associates
  - Marketing
  - Fundraising
  - Sale of PHI
  - Right to request restrictions
  - Electronic access
- HITECH Breach Notification
- HITECH Enforcement

Outline of Topics (cont.)

- GINA Privacy
- Other (non-statutory) Modifications
  - Student immunizations
  - Research
  - Decedents
  - Notice of privacy practices (NPP)

HITECH PRIVACY & SECURITY

OCR 7

Business Associates – Old Rule

- CE must have written contract with BA that requires BA to safeguard PHI and not use or disclose PHI other than as provided by the contract
- Contract must ensure any subcontractors agree to these same restrictions
- BA not directly liable for violations
- CE must act to cure known pattern of BA violations, but not liable for acts of BA (except where BA is an agent and CE fails to have contract or cure known pattern of BA violations)

OCR 8

Business Associates – New Rule

- Contract between CE and BA still required; however, now:
  - BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; directly liable for violations
  - BAs must comply with the use or disclosure limitations expressed in its contract and those in the Privacy Rule; directly liable for violations
- Clarification that BAs are liable whether or not they have an agreement in place with the CE
- If CE delegates Privacy Rule obligation to BA (e.g., providing NPPs to individuals), contract must require BA to perform in compliance with Rule
- Makes CE liable for violations of BA agent, acting within scope of agency (Federal Common Law of Agency)

OCR 9

Business Associate Liability

- Direct liability
  - Impermissible uses and disclosures (including more than minimum necessary)
  - Failure to comply with Security Rule
  - Failure to provide breach notification
  - Failure to provide e-access as provided in BA contract
  - Failure to disclose PHI to HHS for compliance and enforcement
  - Failure to provide HITECH accounting (later – no final rule yet)
- Contractual liability for requirements of the BA contract

**Given the importance of this issue to OCR enforcement, we plan to provide more detailed guidance to assist regional investigators

OCR 10

Business Associates – Subcontractors New Rule

- Subcontractors now defined as BAs – BA liability flows "down the chain"
- Does not change parties to the contracts – CE must have BA contract with its BA, BA must have BA contract with subcontractor, and so forth

OCR 11

Definition of Business Associate – New Rule

- Now expressly in definition:
  - Health Information Organizations, E-Prescribing Gateways, others that provide
    - Data transmission services with respect to PHI and
    - Require access on a routine basis to such PHI
  - PHR vendors that provide services to individuals on behalf of covered entities
- Clarification that conduit exception does not apply to BAs that store PHI

OCR 12

Marketing – Old Rule

- Marketing requires written authorization
- Certain communications about health-related products or services by covered entities to individuals not considered marketing
- Face to face marketing communications and promotional gifts of nominal value permitted without authorization

OCR 13

Marketing – New Rule

- Communications about health-related products and services by covered entity to individuals now marketing and require authorization if paid for by third party
- Limited exception for refill reminders (and similar communications)
  - Payment must be reasonably related to cost of communication
- Face to face marketing communications and promotional gifts of nominal value still permitted without authorization

OCR 14

Fundraising – Old Rule

- CE permitted to use demographic information (includes insurance status) and dates of service to fundraise to individuals for its own benefit
- Each solicitation must describe how individual can opt out of future solicitations
- If individual opts out, CE must make reasonable efforts to honor opt out

OCR 15

Fundraising – New Rule

- CE may also use department of service, treating physician, and outcome information to fundraise
- Each communication to individual must include "clear and conspicuous" opt out – no undue burden or more than nominal cost to exercise
- CE may not condition treatment or payment on individual's decision
- CE must honor opt out (no further fundraising communications permitted)
- Flexibility provided in scope of opt out and method to opt back in permitted

OCR 16

Sale of PHI – Old Rule

- CE prohibited from "selling" patient information; however, no general prohibition on receiving remuneration for disclosure of PHI that is otherwise permissible

OCR 17

Sale of PHI – New Rule

- Even where disclosure is permitted, CE is prohibited from disclosing PHI (without individual authorization) in exchange for remuneration
  - Includes remuneration received directly or indirectly from recipient
  - Not limited to financial remuneration
- If authorization obtained, authorization must state that disclosure will result in remuneration

OCR 18

Sale of PHI – New Rule

- Exceptions:
  - Treatment & payment
  - Sale of business
  - Remuneration to BA for services rendered
  - Disclosure required by law
  - Public health
  - Research, if remuneration limited to cost to prepare and transmit PHI
  - Providing access or accounting to individual
  - Any other permitted disclosure where only receive reasonable, cost-based fee to prepare and transmit PHI

OCR 19

Right to Request Restrictions – Old Rule

- Individual has right to request restriction on TPO (and certain other) uses/disclosures
- CE need not agree, but if it does, then bound by restriction

OCR 20

Right to Request Restrictions – New Rule

- CE must agree to individual's request to restrict disclosure of PHI to health plan if:
  - PHI pertains solely to health care for which individual (or person on behalf of individual other than health plan) has paid CE in full out of pocket
  - Disclosure is not required by other law
- CE encouraged, but not required, to notify downstream providers of restriction
- Preamble provides guidance on scope of restriction & other potential implementation issues

OCR 21

Electronic Access – Old Rule

- If individual requests e-copy of PHI in designated record set, CE required to provide the e-copy to the extent it is readily producible
- CEs permitted to charge reasonable, cost-based fee to cover providing the copy (including supplies and labor)
- CE must act on request within 30 days (60 days if PHI is not maintained or accessible to CE on-site)
  - One 30-day extension permitted if CE informs individual in writing of need for delay

OCR 22

Electronic Access – New Rule

- If individual requests e-copy of PHI maintained electronically in designated record set, CE:
  - Must provide access in electronic form/format requested, if readily producible, otherwise in readable electronic form/format as agreed to by CE and individual
- If requested, CE must transmit copy of PHI to individual's designee (not limited to electronic access)
  - Request must be in writing & signed
  - Must clearly identify designated person and where to send

OCR 23

Electronic Access – New Rule

- Clarifies CE may charge for:
  - Labor for copying
    - Time attributable to reviewing request and producing copy
  - Cost of electronic media
    - CD, USB drive, or similar portable media/device, if individual requests copy on portable media
- CE has 30 days (with one 30-day extension) to act on request for access
  - Provision allowing initial 60 days for off-site PHI removed

OCR 24

BREACH NOTIFICATION

OCR 25

Definition of Breach – Old Rule

- Impermissible use or disclosure of (unsecured) PHI which compromises the security or privacy of the information
  - Compromises means poses a significant risk of financial, reputational, or other harm to the individual
- To determine if must notify, preamble stated CE/BA must perform risk assessment, based on at least:
  - What type or amount of PHI was used or disclosed
  - Who received/accessed the information
  - Potential that PHI was actually accessed or acquired
  - What steps were taken to mitigate
- Exceptions for inadvertent, harmless mistakes
- Narrow exception for limited data sets without dates of birth & zip codes

OCR 26

Definition of Breach – New Rule

- Harm standard removed
- Impermissible use/disclosure of (unsecured) PHI *presumed* to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least the following:
  - Nature & extent of PHI involved
  - Who received/accessed the information
  - Potential that PHI was actually acquired or viewed
  - Extent to which risk to the data has been mitigated
- Exceptions for inadvertent, harmless mistakes remain
- Exception for limited data sets without dates of birth & zip codes removed

OCR 27

Breach Notification

- Makes permanent the notification and other provisions of August 2009 interim final rule, with only minor changes/clarifications, e.g.,
  - Clarifies that notification to Secretary of smaller breaches to occur within 60 days of end of calendar year in which breaches were *discovered* (versus *occurred*)

OCR 28

ENFORCEMENT

OCR 29

Enforcement

- Makes permanent the changes from the October 2009 interim final rule
  - New CMP structure
  - Revised limitations on the Secretary's authority to impose CMPs

OCR 30

Enforcement

- Willful neglect
  - Old Rule
    - OCR's investigation of complaints/compliance reviews discretionary, regardless of nature of violation
    - OCR required to attempt to resolve indications of noncompliance by informal means
  - New Rule
    - OCR will investigate or initiate compliance review whenever preliminary review indicates possible violation due to willful neglect
    - Makes discretionary the resolution by informal means, thereby enabling OCR to proceed immediately to penalties (such as in willful neglect cases)

OCR 31

Enforcement

- Definition of Reasonable Cause
  - Old Definition
    - Circumstances that would make it unreasonable for the CE, despite the exercise of ordinary business care and prudence, to comply
  - New Definition
    - Act or omission in which a CE (or BA) knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but in which the CE (or BA) did not act with willful neglect
    - Prevents a gap in penalty scheme

OCR 32

Enforcement

- Factors in Determining the Amount of a CMP
  - Old Rule
    - Secretary has discretion with respect to whether and how to apply list of mitigating/aggravating factors in determining CMP amount
  - New Rule
    - Secretary required to base her determination on nature and extent of the violation and extent of the harm resulting from the violation
- Affirmative Defenses
  - Old Rule
    - No CMP where a violation is criminally punishable
  - New Rule
    - No CMP where a violation is criminally punished

OCR 33

GINA

GINA

- Old Rule
  - Genetic information considered PHI to the extent it is identifiable and maintained by CE (or BA)
- New Rule
  - Expressly provides that "genetic information" is PHI
  - Prohibits the use or disclosure of genetic information for underwriting purposes by all health plans, except long-term care plans
  - Terms and definitions track regulations prohibiting discrimination in health coverage based on genetic information

OTHER MODIFICATIONS

Student Immunization Records

- Old Rule
  - Authorization generally required to disclose proof of student immunization to school
- New Rule
  - CE may disclose proof of immunization of child to schools in States with school entry laws
  - Written authorization not required
  - Need prior oral or written agreement from parent or guardian
  - Must document agreement

Research Authorizations – Old Rule

- Compound Authorizations
  - Not permitted for use/disclosure of PHI for conditioned and unconditioned research activities (e.g., separate authorization forms required for use/disclosure of PHI in a clinical trial and storage of PHI in a biorepository)
- Future Use Authorizations
  - Not permitted; authorizations for research must include descriptions that are study specific

Research Authorizations – New Rule

- Compound Authorizations
  - Single authorization form permitted for use/disclosure of PHI for conditioned and unconditioned research activities, with clear opt in for voluntary (unconditioned) component
  - Flexibility permitted on ways to differentiate the components
- Future Use Authorizations
  - Permitted so long as authorization for future research purposes adequately describes such purposes such that it would be reasonable for the individual to expect his or her PHI could be used or disclosed for the research
- Aligns with Common Rule informed consent requirements

Decedent Information

- Old Rule
  - Health information about decedents generally protected in same manner/extent than that of living individuals
  - CE may disclose PHI to family members & others involved in care; application to decedent PHI unclear
- New Rule
  - Decedent's information is no longer PHI after 50-year period
  - CE may disclose decedent's PHI to family members and others who were involved in care/payment for care of decedent prior to death, unless inconsistent with prior expressed preference

OCR 40

Notice of Privacy Practices – Old Rule

- Must describe uses and disclosures of CE, CE's legal duties and privacy practices, and individual rights
- When there is a material change to NPP, health plans must provide revised notice to individuals covered by the plan within 60 days of material revision

OCR 41

Notice of Privacy Practices – New Rule

- Content must now include:
  - Statements regarding sale of PHI, marketing, and other purposes that require authorization
  - Statement that individual can opt out of fundraising communications
  - Statement that CE must agree to restrict disclosure to health plan if individual pays out of pocket in full for health care service
  - Statement about individual's right to receive breach notifications
  - For plans that underwrite, statement that genetic information may not be used for such purposes
- Health plans may distribute materially revised NPPs:
  - By posting on web site by effective date of change and including in next annual mailing to individuals; or
  - Mailing to individuals within 60 days of material revision.

OCR 42