



Analysis of the Proposed Rule, May 31, 2011, HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act (HITECH)

On Tuesday, May 31, 2011, the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) published its long anticipated Notice of Proposed Rulemaking (NPRM) for modifications to the HIPAA privacy rule as amended by Title XIII of the HITECH Act (part of the 2009 American Recovery and Reinvestment Act (ARRA), 45 CFR Part 164, RIN: 0991-AB62.

An electronic copy of this NPRM rule can be found on the electronic Web pages of the *Federal Register* at http://www.access.gpo.gov/su_docs/fedreg/a110531c.html, beginning on page 76FR31426. Go to the Health and Human Services Department category for the NPRM which can be downloaded in either text or PDF format.

This NPRM was superseded by a request for information from the OCR on May 3, 2010. AHIMA responded to that request and the AHIMA response can be found at the AHIMA Advocacy and Policy Website <http://www.ahima.org/advocacy>.

Key Highlights of the OCR Notice of Proposed Rulemaking

- **HIPAA Accounting for Disclosure Rule is revised to accommodate HITECH requirement for electronic disclosure of treatment, payment, and healthcare operations.**
- **Several Disclosure accounting requirements are also modified to simplify and better specify the situations that must be included in an accounting.**
- **Based on HITECH legislation and HIPAA authorization OCR also proposes an Accounting of Access – access to electronic designated record sets and not limited to an “EHR.”**
- **Due to the requirements for accounting, the Notice of Privacy Practices (NPP) will require Covered Entities to reissue their NPP.**
- **Compliance with the disclosure final rule will be 240 days after publishing.**
- **Compliance with the access report for electronic designated record sets obtained after January 1, 2009 is extended to January 1, 2013. Compliance for systems obtained before January 1, 2009 is proposed for January 1, 2014.**

Response Dates

Responses to this NPRM are due no later than August 1, 2011. Instruction on the various ways to submit comments are contained in the NPRM on page 76FR31426.

NOTICE: *This review of the NPRM HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act is intended as an overview of the NPRM and not as a complete detailed analysis of the rule. Readers seeking to respond to the*

rule are encouraged to read the entire proposed rule and not rely on this or any other summary of the rule. AHIMA will be responding to this within the allotted timeframe and will publish its comments on the AHIMA website.

Summary (76FR31426)

OCR states that the purpose of these modifications is, in part, to implement the statutory requirement under HITECH which requires covered entities (CEs) and business associates (BAs) to account for disclosures of protected health information (PHI) to carry out treatment, payment, and healthcare operations (TPO) if such disclosures are through an electronic health record (EHR). OCR also announces that pursuant to both HITECH and under its general authority given by HIPAA, it also proposes to expand the accounting provision to provide individuals with the right to receive “an access report indicating who has accessed electronic protected health information in a designated record set.”

I. Statutory and Regulatory Background (76FR)

A. The Accounting of Disclosures under the Current Privacy Rule

This discussion notes the current requirements under HIPAA before the HITECH requirements are in place:

- As current rules for the accounting of disclosures under HIPAA administrative simplification, Pub. L. 104-191;
- As current rules that apply to HIPAA CEs and BAs;
- With the definition of “disclosure” as (§160.103): “the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information;”
- With regard to research issues; and
- Limited in defining paper versus electronic requirements under HIPAA.

B. Changes Required by HITECH (76FR31427)

This section discusses highlights of the requirements from the HITECH legislation including:

- The requirement that disclosure to carry out treatment, payment, and healthcare operations are no longer exempt from a report of disclosures if disclosure is made through an electronic health record;
- Shortening the accounting of disclosure requirement to disclosures made during the three years prior to the request;
- Requiring, in situations where a BAs makes a disclosure via an EHR for purposes of treatment, payment, and health care operations on behalf of the CE, to either be included in the report on disclosure by the CE, or for the CE to provide requestor with a list of all BAs in the requested time period [this is later changed in the requirements];
- The requirement that HHS promulgate regulations governing what information is to be collected about the disclosures taking into account the interests of the individual versus the administrative burden on the provider of the accounting;
- The specific requirements for an accounting of disclosures accounting regulation and certification criteria; and
- The compliance date requirements for the rule specifying that “HIPAA CEs that have acquired an EHR after January 1, 2009 is January 1, 2011, or the date that it acquires an EHR, whichever is

later. For CEs that acquired EHRs prior to January 1, 2009, the effective date is January 1, 2014. The statute authorized the Secretary to extend both of these compliance deadlines to no later than 2013 and 2016, respectively.”

II. Request for Information (76FR31427)

In May of 2010, OCR put out a request for information that included nine questions related to HIPAA CEs, individuals, and the current HIPAA and HITECH requirements related to accounting of disclosures. The published section provides a description of the questions and a breakdown of some of the responses. [AHIMA responded to these questions – see AHIMA’s comments at www.ahima.org/advocacy.]

III. Overview of Proposed Rule (76FR31428)

OCR notes that it is revising §164.528 of the HIPAA Privacy Rule into two separate rights for individuals:

Individual’s right to an accounting of disclosures (a)

- Revisions to §164.528’s disclosure requirements is based on general authority under HIPAA.
- The right to an accounting of disclosures is not expected to include additional information about the disclosure of designated record set information (whether hard-copy or electronic) to persons outside the CE and its BAs for certain defined purposes.
- The intent of the accounting of disclosures is to provide more detailed information (a “full accounting”) “for certain disclosures that are most likely to impact the individual.”
- The disclosure accounting is seen as somewhat of a “manual, expensive, and time consuming process...”
- The right encompasses disclosure of both hard copy and electronic PHI that is maintained in a designated record set. CEs would be expected to report both their own disclosures as well as those of its BAs.
- The accounting covers three years.
- The NPRM proposes that compliance with accounting of disclosures changes occur 180 days after the effective date of the final rule, which under HIPAA requires 60 days added by Congress and is therefore 240 days after the final rule is published in the *Federal Register*.

Individual’s right to an access report (“which would include electronic access by both workforce members and persons outside the covered entity”) (b)

- The right to an access report is based in part on the requirement of section 13405(c) of HITECH to provide individuals with information about disclosure through an EHR to treatment, payment, and healthcare operations. OCR indicates the access report is also based on its general authority under HIPAA, “in order to ensure that individuals are receiving the information that is of most interest.”
- The right is expected to provide information on who has accessed electronic PHI in a designated record set(s), including for purposes of treatment, payment, and health care operations.
- The access report is intended to allow individuals to learn if specific persons have accessed their electronic designated record set information.
- The access accounting is seen as a “more automated process that provides valuable information to individuals with less burden...”

- “By limiting the access report to electronic access, the report will include information that a CE is already required to collect under the Security Rule (§164.308(a)(1)(ii)(D) and §164.312(b)).”
- The right only applies to PHI about an individual that is maintained in an electronic designated record set and does not distinguish between “uses” and “disclosures.”
- The accounting covers three years.
- The access report is to include date of access, time of access, and name of the person (or name of the entity if the person’s name is unavailable) who accessed the information, and if known, a description of the PHI accessed.
- The NPRM proposes that compliance with accounting for access by CEs and BAs should occur as follows:
 - Provide individuals with a right to an access report beginning January 1, 2013 for electronic designated record set systems acquired after January 1, 2009.
 - Provide individuals with a right to an access report beginning January 1, 2014 for electronic designated record systems acquired as of January 1, 2009. [The assumption is that these systems will require more retrofitting than newer systems.]

The two rights are seen as complimentary and attempting to “shift the accounting provision from a manual process that generates limited information to a more automated process that produces more comprehensive information...”

Notice of Privacy Practices (NPP)

The two rights will patently also affect the revision to the requirements for notices of privacy practices (NPP).

IV. Section-by-Section Right to an Accounting of Disclosures (76FR31429)

Note: When commenting on the NPRM identify the section you are commenting on. It is also helpful to note the page and column where the issue you are addressing appears. This makes your comments more useable for OCR review.

A. Accounting of Disclosures of Protected Health Information - § 164.528 (a)

Here OCR notes that its reasons for revision are to improve workability of the requirements and provide the individual with information most likely to impact him or her.

1. Standard: Right to Accounting of Disclosures (76FR31429)

OCR notes the changes that it is proposing to the right for an accounting of disclosures:

- The scope of the information subject to the accounting about an individual in a designated record set would explicitly include BAs.
- The accounting period would be changed from six years to three years.
- A list of the types of disclosures that are subject to the accounting would be given, rather than listing the types of disclosures that are exempt from the accounting.
- The accounting is limited to protected health information about the individual in a designated record set. Designated record sets include the medical and health care payment records maintained by or for a CE, and other records used by or for the CE to make decisions about individuals. (§164.501)

- OCR believes that the changes above would align the accounting provision with the individual's right to access and amend PHI, which are limited to PHI in a designated record set.
- OCR (76FR31430) sites an example of information that would fall outside of the accounting; in this case a file used for improving patient care across the entity.
- OCR notes, and it is worth repeating, that PHI anywhere is still subject to the Privacy and Security Rules. Further, the HITECH Breach Notification requirements also apply to all PHI wherever it exists in the CE or BA.
- Paragraph (a)(1)(i) would be changed to address which disclosures are subject to the accounting requirement. OCR believes this will make the rule easier to follow and understand.
 - CEs are still required to account for disclosures that are impermissible under the privacy rule.
 - If a disclosure has been identified through a breach notification, it need not be included in the accounting if occurring within the three year period.
 - Disclosures for the following will need to have an accounting:
 - Public health – except those situations involving reports of child abuse or neglect or situations where the reporting is known to be required by law such as communicable disease;
 - Judicial and administrative proceedings;
 - Law enforcement activities;
 - Situations to avert a serious threat to health or safety;
 - Military and veterans activities;
 - Department of State's medical suitability determination;
 - Government programs providing public benefits;
 - Workers' compensation.
 - The follow disclosures continue to be excluded from the accounting requirement:
 - To individuals of PHI about them;
 - Incident to a use or disclosure otherwise permitted or required by the Privacy Rule;
 - Pursuant to an authorization;
 - For the facility's directory;
 - To persons involved in the individual's care;
 - For national security or intelligence purposes;
 - To correctional institutions;
 - To law enforcement officials who have a prisoner in custody;
 - As part of a limited data set; and
 - When disclosure for treatment, payment and health care operation associated with paper records.
 - OCR provides considerable discussion (76FR31432-33) on its thoughts regarding lifting the current HIPAA requirements associated with research. The Office cites a number of problems that have occurred in the administration of these requirements and recommendations from groups such as the Institute of Medicine (IOM) suggest that the risk to privacy is very small compared to the administrative burden. OCR notes that an individual will still be able to request an access report from the CE, which would include access for research purposes from the designated record sets.
 - OCR also proposes (76FR31433) to exclude most disclosures that are required by law because the disclosures are usually population based and not concerning a specific individual, however CEs and BAs must account for disclosures for judicial and administrative proceeding and for law enforcement purposes, even when such disclosures are required by law. This requirement continues under OCR's belief that disclosures for

law enforcement purposes and judicial and administrative proceedings directly implicate an individual's legal and/or personal interests and individuals should have a right to learn of such disclosures.

- (76FR31414) If a CE has been subject to the Privacy Rule for less than three years, then the CE only need account for the period of time during which the CE was subject to the Rule.

OCR requests comment on this section's proposals:

- Are there unintended consequences with limiting accounting to PHI in designated record sets in terms of workability or the privacy interest of the individual?
- Are there concerns with limiting the accounting for three years?
- Are there burdens on CEs and benefits to individuals associated with also receiving an accounting of disclosures that includes information provided in accordance with the breach notification requirement?
- Are there other categories of public health disclosures that warrant an exception because such disclosures may be of limited interest to individuals and/or because accounting for such disclosures may adversely affect certain population-based public health activities such as active surveillance programs?
- What is the complexity of carving out such public health disclosures – would it lead to too much confusion among individuals and CEs?
- Should exemption include accounting requirements for certain categories of disclosures that are currently subject to disclosure including
 - Victims of abuse, neglect, or domestic violence;
 - Health oversight activities;
 - Research purposed;
 - Decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye, or tissue donation;
 - Protective services for the president and others; or
 - Disclosures required by law including to the Secretary to enforce HIPAA? [OCR rationale can be found on 76FR31432.]
- Public comment is solicited on the value of the current accounting for research disclosures to individuals who have used or might in the future request such an accounting, including comments on what may be the most important /useful elements of the current accounting to individuals.
 - OCR also asked CEs to provide data regarding the number of protocols that would typically be included in a protocol listing, the nature and number of smaller research studies that involve the disclosure by the CE of PHI about less than 50 individuals and for which a specific, accounting is currently and the burdens on researchers and CEs to provide the requested accountings of disclosures.

2. Implementation Specification Content of the Accounting (76FR31433)

OCR makes a number of proposed modifications to the implementation specifications and provides rationale that will not be repeated here. The proposed modifications include:

- A CE or BA need only provide an approximate date or period of time for each disclosure, if the actual date is not known.
 - At a minimum, the approximate data must include a month and year or a description of when the disclosure occurred from which an individual can readily determine the month and year of the disclosure.

- For multiple disclosures to the same person or entity for the same purpose, the approximate period of time is sufficient.
 - Note that under this proposal, a time period of multiple months is permitted for multiple disclosures to the same recipient for the same purpose, but not a single disclosure.
- OCR further clarifies that the date of disclosure may be descriptive, rather than a specific date.
 - For example, the accounting may provide that a disclosure to a public health authority was “within 15 days of discharge” or “the fifth day of the month following discharge.”
- The accounting must include the name of the entity or natural person who received the PHI, and if known, their address.
 - OCR is proposing an exception for when providing the name of the recipient would itself represent a disclosure of PHI about another individual. OCR provides an example of a breach situation where this might occur.
- A revision that makes a slight revision to the regulatory language, replacing “a brief description of the PHI disclosed” with “a brief description of the type of PHI disclosed.”
 - Likewise a revision changing the language in the accounting description from “statement” to “description” to make clear that only a minimum description is required if it reasonably informs the individual of the purpose.
- Requiring CEs to provide individuals the option of limiting the accounting to a particular time period, type of disclosure, or recipient.
 - OCR also notes that while an individual may be required to pay for an accounting of disclosure if the CE has already provided the individual with an accounting within the prior twelve months. OCR suggests that the individual should not have to pay for an accounting report that covers a three-year period if the individual is trying to learn of disclosure that occurred over a more limited period of time.

3. Implementation Specification Provisions of Accounting (76FR31435)

OCR proposes three modifications:

- Decreases the permissible response time from 60 days to 30 days;
 - OCR requests comment on whether a shorter 30-day deadline, with a single 30-day extension, will significantly benefit individuals and whether it will place an unreasonable burden on CEs. Specifically, OCR requests comment on how long covered entities have needed to collect information necessary for an accounting (including from BAs) and to generate an accounting of disclosure. OCR is suggesting by cutting the time period for a request to three years the time to respond should also be less.
- Requires that CEs provide individuals with the accounting in the form and format requested by the individual if readily producible.
 - There is additional discussion (76FR31455), but this is a requirement that is now surfacing in a number of other requirements including Meaningful Use.
- Clarifies that the CE may require the individual to submit the accounting requests in writing.
 - OCR suggests that CEs might want to have a form for this request and that having such a request might help to focus the request to a shorter time period.

4. Implementation Specification: Law Enforcement and Health Oversight Delay (76FR31435)

While OCR is retaining the requirement for CEs to delay the provision of an accounting of disclosures based on an ongoing law enforcement investigation, it is also proposing to no longer include a delay

for a health oversight investigation since it is also proposing that disclosure for health oversight activities are no longer subject to the accounting requirements.

5. Implementation Specification: Documentation (76FR31436)

This specification requires close reading. Essentially, ONC indicates that a CE must:

- Maintain the documentation necessary to generate an accounting of disclosures for three years,
- Retain a copy of any accounting that was provided to an individual for six years from the date the accounting was provided, and
- Retain documentation of the designation of who is responsible for handling accounting requests for six years from the last date the designation was in effect.

Rationale for these recommendations is provided. CEs may want to comment on the requirements as stated.

B. Right to an Access Report -- § 164.528(b) (76FR31436)

1. Standard: Right to an Access Report (76FR31436)

In addition to the right to an accounting of disclosures, OCR is proposing to provide individuals with a right to receive an access report that indicates who has accessed their electronic designated record set information. This new right does not extend to access to paper records.

- OCR defines “access logs” and “access reports” in its discussion:
 - The access log is the raw data that an electronic system containing PHI collects each time a user accesses information. (May also be referred to as an “audit trail” or “audit log.”)
 - The access report is a document that a system administrator or other appropriate person generates from the access log in a format that is understandable to the individual. (May also be referred to as an “audit report.”)
- OCR indicates that its expectation is that data from each access log will be gathered and aggregated to generate a single access report (including data from BAs’ systems.)
- OCR notes that while HITECH only addresses “disclosures and refers to an EHR, OCR is exercising its discretion under HIPAA to expand the right to uses of information and to all electronic PHI about an individual in any designated record set. OCR reiterates that this only addresses electronic PHI and therefore the access report will not capture treatment, payment, and healthcare operations information that are disclosed outside of the electronic designated record set.
- OCR is proposing this right because it believes that:
 - Individuals are interested in learning who has accessed their information without regard to whether the access is internal (a use) or by a person outside the CE and its BAs (a disclosure).
 - Inclusion of both uses and disclosures in the access report significantly increase the benefits to individuals by providing a more complete picture of who has accessed their information.
 - Inclusion of “uses” of the designated record set information does not represent an unreasonable burden on CEs and BAs and actually may lessen the burden of the CE or BA since they do not have to determine “use” from “disclosure.”
 - Including all electronic PHI in a designated records set, rather than only EHR information, improves transparency and better facilitates compliance and enforcement since the Security Rule already requires access logs.
 - By only requiring access to electronic PHI, the burden on CEs and BAs will be reduced.

- By taking the broader approach and using designated records sets, it can avoid the need to categorize certain electronic systems as EHRs.
- OCR is proposing the requirement for an access report to both CEs as well as BAs that maintain designated records set information.
 - OCR notes that a CE only needs to obtain information from BAs that handle electronic designated records set information, which should lessen the burden. OCR also notes that BAs should be maintaining the necessary information both under the HIPAA Security Rule and the expansion of HIPAA to BAs under HITECH.

2. Implementation Specification: Content of the Access Report (76FR31437)

OCR is proposing that an access report include:

- Date of access;
- Time of access;
- Name of the natural person, if available, otherwise the name of the entity accessing the electronic designated records set information;
- Description of what information was accessed, if available; and
- Description of the action by the user, if available (e.g. “create,” “modify,” “access” or “delete”).

In describing the items the report must contain, OCR makes comments including:

- Its intention for the CE to include the start time in the access report, “although CEs are free to also include the end time when it is available.”
- That CEs or BAs may rely on a user ID; however, a CE must be able to readily match a user ID with a first and last name when a report is requested.
- “Permit[ing]” when access is from another electronic system, the access log to identify such access with the name of the CE in order to reflect that the individual’s information was accessed by one of the CE’s systems.
- Its intention that the access report includes a description of what information in the electronic designated records was accessed – if the information is available.
- Not requiring CEs and BAs to include in the access report a description of what use or disclosure was ultimately made with the information accessed or to whom the user provided the information.
- Its recognition that there might be multiple designated record systems and therefore multiple access logs and that while this information should be collected now under HIPAA requirements, the aggregation could be a burden, which it believes is reasonable given the benefit to the individual.
- Its recommendation that CEs offer individuals the option to limit the access report to specific organizations or individuals that are of interest to the requesting individual.

OCR request comments on the following questions on this implementation specification:

- What is the burden of providing identifying information about internal systems (making access) and the interests of individuals in learning of such internal changes?
- What is the availability of the information on what PHI information was accessed in current access logs, and
 - what is the importance of the this access information to individuals, as well as
 - the potential administrative burden of requiring that access reports include a description of what information was accessed?

- Do the (current) access logs provide a description of the information that was accessed? What is the administrative burden potential for providing this descriptive information?
- While the proposed rule does not require an address of the user, what is the potential burden to CEs and potential benefit to individuals of requiring the access report to include address information that indicates where the access occurred?
- The proposed rule does not require CEs or BAs to include a description of the purpose of access in access reports, but OCR is requesting comments on this approach. OCR also asks for comment on its assumption that systems do not record information about the purpose of the access and ultimate recipient of the information within audit logs.
- OCR also asks for comments on ways in which such accesses, if accepted from the access report, could be identified and excluded in an automated way?
- OCR asks if its assumptions on the burden of aggregating multiple access reports for one individual is correct.

3. Implementation Specification: Provision of the Access Report (76FR31440)

OCR makes the following proposals:

- A CE will have 30 days to provide the access report including the logs of BAs that create, receive, maintain or transmit electronic designated record set information.
- A CE may extend the time by 30 days where necessary, as long as the CE provides the individual with a written statement that includes the reason for the delay and the day by which the CE will provide the access report. The CE is only permitted one extension of time.
- A CE must provide the access report in the machine readable (digital information stored in a standard format enabling the information to be processed and analyzed by computer) or other electronic form and formation requested by the individual, if it is readily producible in such form and format, or as agreeable to by the CE and the individual. If not agreeable then hard copy is acceptable. Hard copy, rather than electronic, is also acceptable if requested by the individual.
- The first access report must be given at no charge in a 12 month period and subsequent copies can be charged if individuals are notified of such.
- Requests can be required in writing.

4. Implementation Specification: Documentation (76FR31440)

OCR is proposing the same documentation requirements for access reports as for accountings of disclosures. (See above.)

5. Accounting of Disclosures That Are Made Through Electronic Health Information Exchange (76FR31440)

This section is an interesting discussion on the part of OCR regarding its current decision not to require an accounting of disclosures for treatment, payment, or operations via a health information exchange (noun). OCR concludes that the burden at this time would be much higher than the benefit to the individual; however, OCR reminds CEs and BAs that:

- Individuals still have a right to learn of disclosures through a electronic health record exchange (verb), and
- Each time electronic designated records set information is accessed for purposes of electronic health information exchange (verb), regardless of the purpose of the exchange, the date, time, and identity of the user will be captured in the access report.

C. Confidentiality of Patient Safety Work Product (76FR31441)

OCR proposes to note that a covered entity must exclude from an accounting or access report any information that meets the definition of patient safety work product. This is to avoid any conflicts between the HIPAA and proposed modifications and the regulations established under the Patient Safety and Quality Improvement Rule.

D. Notice of Privacy Practices -- §164.520 (76FR31441)

OCR reiterates the HIPAA requirements when privacy practices change as they do here with the accounting of access, therefore requiring a revised Notice of Privacy Practices (NPP). OCR also notes that the earliest requirement for change is potentially January 1, 2013. OCR suggests that this requirement is much easier for healthcare providers because they maintain a one-to-one relationship with the individual. Health plans are another story and OCR notes a number of considerations it is considering for the final rule. OCR also makes some suggestions that health plans might consider and essentially is asking for comment on what it might require in the final rule for health plans. This does not preclude comments on the requirements impact on healthcare providers or other CEs or BAs.

V. Effective and Compliance Dates (76FR31441)

OCR is proposing separate compliance dates for the changes to the accounting of disclosures requirements and for the right to receive an access report.

Accounting of Disclosures Report

Taking into account the HIPAA law, the compliance date for the revised accounting of disclosures requirements will occur 240 days after the final rule is posted in the *Federal Register*. OCR does not see any reason for this time line to be extended.

Accounting of Access Report

Subject to HITECH, OCR is proposing two different compliance dates depending on the access of an electronic designated records set.

- If the electronic designated records set has been obtained after January 1, 2009, OCR has taken the liberty afforded by HITECH to propose January 1, 2013, for the access report compliance date. This is an extension of two years from the HITECH date set in legislation.
- If the electronic designated records set was obtained on or prior to January 1, 2009, OCR is proposing the legislated compliance date of January 1, 2014 be retained and is not extending it as permitted.
- OCR is encouraging CEs and BAs during 2013 to provide access reports that include all designated records set systems even if the CE or BA is not required to include some of the electronic systems at that time.
- OCR is maintaining the requirement of a three-year period to be covered by requests given the current HIPAA Security Rule requirements. OCR is requesting comment on whether CEs will be able to generate access reports covering the preceding three years on these compliance dates.

OCR does not address the difficulty of determining the dates associated with obtaining a variety of systems that may make up an entity's electronic designated records set. This may be an area for comment.

VI. Regulatory Analyses (76FR31442)

A. Introduction

This section notes the requirements for a regulatory impact statement that accompany all NPRMs.

1. Executive Order 12866 (76FR31442)

Under the executive order, OCR notes that this rule has been designated a “significant regulatory action” although not economically significant. The latter avoids a regulatory impact analysis, however OCR notes that it has requested input on the impact of these rules. OCR sees most of the costs associated with new NPPs at approximately \$20.2 million.

OCR requests more information on:

- The number of anticipated accounting of disclosures and access reports;
- The additional costs, if any, of offering them in electronic formats (both machine readable or non machine readable); the burden of tracking access of electronic designated records set information; and any other additional changes to existing systems that would be necessary.

2. Regulatory Flexibility Act [76FR31442]

OCR requests comment on the number of small entities in the health insurer and health plan administrator market as required by the RFA. It notes that all providers are considered small entities.

3. Unfunded Mandates Reform Act [76FR31443]

OCR must analyze if the NPRM will exceed a certain amount of spending on state, local, or tribal governments – an unfunded mandate. OCR responds by noting that it does not estimate such a threshold being met.

4. Federalism [76FR31443]

Similar to the Unfunded Mandate this is another situation where OCR must register impact on the states. OCR notes that parts of HIPAA can be preempted by states and again reiterates that it does not see this rule as meeting any threshold under Federalism.

B. Why are we [OCR] proposing these regulations? [76FR31443]

OCR notes its obligations under HITECH and goes on to reiterate the benefits to individuals that will be brought about when compliance is met.

1. What are the current regulations? [76FR31443]

OCR cites the HIPAA regulations.

2. What are we proposing? [76FR31444]

OCR reiterates a summary of what is covered above.

3. What would be the impact of changes to accounting of disclosures requirements? [76FR31444]

OCR responds:

- Benefit to individuals by reducing the amount of time it takes for them to receive an accounting.
- Exclusion of a number of categories of disclosures from the accounting.
- Limiting the scope of the accounting will not diminish the benefit because the individual will receive an accounting that is most likely to have an immediate impact on his or her interests.
- Requirements and associated administrative costs on CEs and BAs will be reduced.

OCR requests comments on:

- The cost of the current burden on CEs and BAs associated with the accounting of disclosures especially given the limited number of requests.
- The impact of only permitting a single 30-day extension.

4. *What would be the impact of adding the right to access report?* [76FR31444]

OCR responds:

- Significant benefit to all individuals by providing them a means to learn who has access to their electronic PHI.
- Information required in the report is almost the same as that required by the HIPAA Security Rule.
- CEs additional burden will consist of generating access reports for each electronic designated records set system and aggregating this information into a single electronic access report. This burden will be impacted by the number of requests; however, OCR suggests the cost to generate access reports will be minimal.
- The decrease in the number of days a CE will have to produce a report in a form or format requested by the individual.
- The impact on systems that use IDs rather than the individual accesser's name, with the requirement that the ID be translated to a name. OCR goes on to note that the ability of the CE to suggest a narrower scan could lessen this burden.

OCR requests comments on:

- The number of anticipated access reports, the burden of tracking access to electronic designated records set information, including whether its proposal will have any unintended effects by requiring significant change to existing systems, and the burden caused by generating an access report.
- The additional burden, if any, of providing electronic access reports (either in machine readable or other electronic format).
- The burden of modifying reports to fit a particular time period requested by the individual.

***What alternatives did we consider?* [76FR31445]**

OCR notes alternatives:

- Applying the access report requirements to only disclosure for treatment, payment, and healthcare operations through an EHR.
- Requiring access reports to include the purpose of the disclosure, and notes that while this is not an alternative it chose to require now, it could become a requirement in the future.

C. How much will it cost covered entities to notify individuals of their new privacy rights? [76FR31445]

OCR provides an analysis that suggests the aggregate costs to be approximately \$20 million for all CEs. OCR requests comments on its analysis.

OCR notes that it expects to publish the final rule in late 2011. It does not note that further requirements are forthcoming in HITECH-based HIPAA Privacy and Security Rules (suggested by OCR in the community as coming out in the fall of 2011) that could also impact the change in privacy practices if delayed for any period of time.

OCR indicates that 673, 324 will be affected by the proposed rule.

D. Regulatory Flexibility Analysis [76FR31446]

Using its calculations, OCR suggests that the average cost per CE will be approximately \$30.00.

OCR notes that it has no information on how many ERISA plans self-administer and requests data from the public for further analysis.

VII. Collection of Information [76FR31446]

This section reiterates the NPRM process and in this case how it comes about from HITECH.

PART 164 SECURITY AND PRIVACY [76FR31447-49]

The actual proposed rule only takes two pages (spread over three). It is laid out as it would be super imposed on the existing Part 164. If you have a question on the above discussion, it helps to look at this section to see how it actually is written. It also helps at times to see the existing PART 164. An amalgamated, unofficial copy exists at the OCR Website <http://www.hhs.gov/ocr/privacy>.

AHIMA will be providing comments to this NPRM. When made, comments will be posted to the AHIMA Advocacy and Policy Website at: <http://www.ahima.org/advocacy> under Comments and Testimony.

AHIMA is the premier association of health information management (HIM) professionals. AHIMA's 61,000 members are dedicated to the effective management of personal health information needed to deliver quality healthcare to the public. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning. To learn more about the association, go to www.ahima.org.