



33 W. Monroe Street
Suite 1700
Chicago, IL 60603-5616
Tel 312 664 4467
Fax 312 664 6143
www.himss.org

1 August 1, 2011

2
3 Ms. Georgina C. Verdugo, JD, LLM, MPA
4 Director
5 Office of Civil Rights
6 U.S. Department of Health and Human Services
7 200 Independence Avenue, SW
8 Washington, DC 20201
9

10 Dear Director Verdugo:

11
12 HIMSS appreciates this opportunity to comment on the Notice of Proposed Rulemaking
13 (NPRM), “HIPAA Privacy Rule Accounting of Disclosures Under the Health Information
14 Technology for Economic and Clinical Health Act (76(104), pp. 31426-31449),” published in the
15 Federal Register by the Department of Health and Human Services (HHS) Office of Civil Rights
16 (OCR) on May 30, 2011. This NPRM implements the provisions of Section 13404 (e) of the
17 American Recovery and Reinvestment Act (ARRA) Health Information Technology for
18 Economic and Clinical Health (HITECH) Act.

19
20 HIMSS is a cause-based, not-for-profit organization exclusively focused on providing global
21 leadership for the optimal use of information technology (IT) and management systems for the
22 betterment of healthcare. Founded 50 years ago, HIMSS and its related organizations have
23 offices in Chicago, Washington, DC, Brussels, Singapore, Leipzig, and other locations across the
24 United States. HIMSS represents more than 37,000 individual members, of which two-thirds
25 work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes
26 over 500 corporate members and more than 120 not-for-profit organizations that share our
27 mission of transforming healthcare through the effective use of information technology and
28 management systems. HIMSS frames and leads healthcare practices and public policy through its
29 content expertise, professional development, and research initiatives designed to promote
30 information and management systems contributions to improving the quality, safety, access, and
31 cost-effectiveness of patient care.

32
33 **HIMSS Summary Comments:**

34 HIMSS appreciates the opportunity to engage with the Office of Civil Rights on requirements for
35 an updated dialogue on the Accounting of Disclosures. We have focused our response on the
36 new patient right to an “Access Report,” and the statutory requirement for OCR to take into
37 account the value of the data to the patient, as well as the burden to the organization to collect
38 data and produce a report (balance test).

39
40 HIMSS appreciates OCR’s attempt to develop a workable compromise to accommodate the
41 desire for transparency for patients, while balancing the burden of CEs and BAs. We are
42 concerned, however, that the proposed solution has several major challenges for stakeholders and
43 their implementation and compliance, These challenges may arise from an incomplete
44 understanding of existing information technologies and their capabilities healthcare

45 organizations to readily comply. They may also come from a possible under-appreciation of the
46 time and facilities burden on CEs and BAs to meet the new requirements. Moreover, the Access
47 Report right proposed for patients in the NPRM may not achieve the goals of creating
48 transparency and clarity for patients who may wish to learn how their clinical information is used
49 and shared.

50
51 HIMSS recommends that the healthcare community and patients alike will benefit from OCR
52 reconsidering its approach and engaging industry experts and patient advocates in further
53 dialogue about the best means for creating a balanced rule. HIMSS also appreciates that the
54 Secretary must resolve how to include the statutorily required Accounting of Disclosures
55 elements relative to Treatment, Payment, and healthcare Operations (TPO), as required by
56 statute, within timelines established by ARRA/HITECH.

57
58 HIMSS intends to work with other healthcare community representative organizations to support
59 the attempt to provide HHS statutory relief from the Accounting of Disclosures TPO inclusion
60 deadlines such that OCR can work with the healthcare community and community-at-large to
61 understand the costs, benefits, and alternatives available for achieving the desired goals.
62 Additional time would afford HHS and healthcare community colleagues the opportunity to
63 capitalize on additional dialog; conduct focus group discussions with technologists and patients
64 to determine the costs and benefits of alternative solutions; and create a balanced approach to
65 achieving transparency for patients.

66
67 If attempts to achieve statutory relief are not successful, HIMSS wishes to point out that the
68 Secretary has authority to promulgate a minimal rule to define what information shall be
69 collected about each disclosure. Importantly, this also means that the Secretary has authority to
70 require *no* specific or particular information about any particular category of uses or disclosures.
71 For example, if there is a category of information that is of limited interest and/or greater burden,
72 it may be possible to account for this category by providing a general explanation of disclosures
73 in that area without accounting for each specific individual access, dates or times. We provide
74 more detailed comments on this matter on lines 529-542

75 76 **Response to Proposed Regulation**

77
78 HIMSS appreciates the opportunity to provide responses to OCR's specific comments from the
79 NPRM that can help foster a solution to meet the needs of patients and healthcare organizations.

- 80
81 1. **[OCR] request[s] comment on our proposal to limit the accounting requirement to**
82 **1. protected health information in a designated record set and**
83 **2. whether there are unintended consequences with doing so either in terms of**
84 **workability or the privacy interests of the individual. (31430)**
85

86 HIMSS appreciates the opportunity to comment on the proposed solution. The use of the
87 Designated Record Set [DRS] concept of accounting has historically focused on limiting the
88 information a person as a patient may request access or amend.
89

90 As currently written the NPRM seems to rely on the assumption that the DRS under the
91 proposed rule applies to a defined data set that “limits” the amount of data or the number of
92 systems involved. Based on our understanding of the current definition for a DRS, the reality
93 is it resides in electronic form in a variety of systems, not simply in an electronic health
94 record as was contemplated by the HITECH Act. If our understanding is correct, then
95 reliance on the DRS may actually become a more burdensome process to access logs and
96 collate information maintained in a variety of electronic systems. Many of these systems
97 simply do not have the capability to collect audit information in this way. In addition, even if
98 each system could collect this information in an audit log, the Access Report requirement
99 also would require log aggregation and analysis functions that currently do not exist in most
100 organizations.

101
102 HIMSS is concerned that the NPRM text implies that OCR has presumed the Access Report
103 requirement places a “reasonable burden” on organizations, yet offers no evidence that it has
104 collected data and conducted an analysis of the burden of this new requirement. HIMSS
105 requests that OCR conduct an analysis of the data contained within the current definition of
106 the DRS, the possible systems involved in the storage of that data, and the issues and burdens
107 with including this data in the Access Report.

108
109 According to feedback from our members, most entities use patient data contained in an EHR
110 to make decisions about the individual and thus it forms a part of the DRS for that patient.
111 Today, some CEs state that such information is not their legally defined medical record since
112 their paper record is their only legal record. So, for these cases, it is only the use of the data
113 that makes it part of the DRS.

114
115 If one were to make a copy of this EHR database and use it exclusively for purposes other
116 than making decisions about the individual (e.g. some program planning purpose – a
117 healthcare operation under HIPAA), then would the access history to this copy be required in
118 the access report under the proposed regulation? If so, then how does such a copy meet the
119 definition of a DRS? If it is not part of the DRS, and not included, then this would not
120 seriously inhibit ability of patients to know who accessed their PHI.

121
122 Consider the same scenario and instead of a copy, the original EHR database that was used
123 and updated as part of the patient care is the data accessed. This includes the data for each
124 individual in the original EHR database, which is certainly used to make decisions about the
125 individual and so clearly fits the DRS definition. HIMSS requests clarification on whether
126 accesses to original data by a CE for a reason not related to making a decision about
127 individuals such as the program planning example will be required in the access report.

128
129 Another example area for consideration and clarification is whether information contained
130 within the database in various medical devices, such as diagnostic, imaging systems or
131 monitors, becomes part of the DRS. This information typically fits the definition of ePHI,
132 can sometimes be accessed on the device for long periods, and is routinely transferred to
133 other systems (e.g. a medical image reporting system) where further access takes place. As a
134 result, access to the ePHI in medical devices seems to fit the DRS definition. The challenge
135 becomes that it is not common for these systems to create access logs. If OCR intends for

136 such medical systems to be covered, then it may be difficult for most CEs to provide access
137 reports, since they may not be able to create access logs. HIMSS appreciates clarification on
138 how the rule should apply in that instance.

139
140 Finally, it is not clear that current audit reports, when applied to certain types of access, such
141 as generation of a report containing multiple names, would readily translate into person-level
142 access reports.

143
144 2. **[OCR does not] believe that it will be a significant detriment to individuals to reduce**
145 **the accounting period from six years to three years. In contrast, we believe it is a**
146 **significant burden on covered entities and business associates to maintain information**
147 **on six years of disclosures, rather than three years. We request comment on this issue**
148 **and if there are specific concerns regarding the need for accounting of disclosures**
149 **beyond three years. (31430)**

150
151 HIMSS is supportive of the NPRM reducing the accounting period for both Disclosure Log
152 Accounting and TPO Accounting to a period of three (3) years. Information about
153 disclosures going back six (6) years is highly unlikely to prove useful or beneficial to the
154 individual.

155
156 In addition, we support the OCR focus for Accounting for Disclosures on a specific list of
157 disclosures, which ends an ongoing source of confusion among covered entities, and is an
158 appropriate way to implement the statutory elimination of the TPO exemption.

159
160 3. **[OCR requests] comment on the burdens on covered entities and benefits to**
161 **individuals associated with also receiving an accounting of disclosures that includes**
162 **information provided in accordance with the breach notification requirement. With**
163 **respect to the remainder of public health disclosures (i.e., public health disclosures**
164 **other than those related to reports of child abuse or neglect), we request comment on**
165 **whether there are other categories of public health disclosures that warrant an**
166 **exception because such disclosures may be of limited interest to individuals and/or**
167 **because accounting for such disclosures may adversely affect certain population-**
168 **based public health activities, such as active surveillance programs. (31431)**

169
170 HIMSS appreciates the opportunity to comment on this area of the NPRM. In the
171 experience of our members, the report of breaches to the individual includes all of the
172 information that would have been contained in an accounting of disclosures. So, there may
173 be little gain to the individual who was notified. Therefore, the organization may be free to
174 include or not include this data in the Accounting of Disclosures.

175
176 However, a person acting as a personal representative for the individual who requests an
177 accounting of disclosures may not have access to the history of breach reports to the
178 individual's data to complement the accounting of disclosures. Thus, personal
179 representatives may be unable to act as competently as required for the individual. It
180 would likely create only a marginal burden for CEs to include these reported breaches in

181 the Accounting of Disclosures, since records of who was notified of any given breach will
182 almost certainly be recorded in a database for a variety of other reasons.

183
184 On a related point, HIMSS requests clarification on whether CEs and BAs would also be
185 free to exclude records of such reported breaches (a type of access) from Access Reports,
186 as this is not clear in the NPRM.

187
188 4. **[OCR] We also request comment on whether the complexity of carving out such**
189 **public health disclosures would lead to too much confusion among individuals and**
190 **covered entities. (31431)**

191
192 HIMSS supports the fact that the NPRM permits CEs to withhold these disclosures from
193 the Accounting of Disclosures.

194
195 HIMSS requests clarification as to whether such disclosures, when executed by accessing
196 an electronic copy of the related PHI, would be required to be included in the Access
197 Report, as this is not clear in the NPRM.

198
199 5. **[OCR also requests] comment on whether the Department should exempt from the**
200 **accounting requirements certain categories of disclosures that are currently subject to**
201 **the accounting. In particular, for the reasons discussed below, we are proposing to**
202 **exclude disclosures about victims of abuse, neglect, or domestic violence under §**
203 **164.512(c); disclosures for health oversight activities under § 164.512(d); disclosures**
204 **for research purposes under § 164.512(i); 1 disclosures about decedents to coroners**
205 **and medical examiners, funeral directors, and for cadaveric organ, eye, or tissue**
206 **donation purposes under § 164.512(g) and (h); disclosures for protective services for**
207 **the President and others under § 164.512(k)(3); and most disclosures that are**
208 **required by law (including disclosures to the Secretary to enforce the HIPAA**
209 **Administrative Simplification Rules). Note, however, to the extent such disclosures**
210 **are made through direct access to electronic designated record set information, such**
211 **disclosures will be recorded and available to the individual in an access report under**
212 **proposed § 164.528(b). (31432) We request comment on our proposal to exclude these**
213 **categories from the accounting of disclosures requirements, including comment on the**
214 **rationales expressed below, and will revisit these exclusions in drafting the final rule**
215 **based on the public comment we receive. (31432)**

216
217 HIMSS appreciates the request for comment, and defers to organizations that have the issue
218 well within their organizational mission.

219
220 6. **[OCR solicits] public comment on the value of the current accounting for research**
221 **disclosures to individuals who have used or might in the future request such an**
222 **accounting, including comments on what may be the most important/useful elements**
223 **of the current accounting to individuals. We also ask covered entities to provide data**
224 **regarding the number of protocols that would typically be included in a protocol**
225 **listing, the nature and number of smaller research studies that involve the disclosure**
226 **by the covered entity of protected health information about less than 50 individuals**

227 **and for which a specific accounting is currently required, and the burdens on**
228 **researchers and covered entities to provide the requested accountings of disclosures.**
229 **(31433)**

230
231 HIMSS supports the NPRM provision that permits the CE to provide a list of research
232 protocols rather than specific information about each disclosure. This relieves significant
233 burden for CE and BA organizations.

234
235 7. **[OCR requests] comment on this proposal. Because we believe it is reasonable to**
236 **assume that individuals are aware that their health information will be disclosed**
237 **where mandated by law. Further, individuals are generally informed that a covered**
238 **entity may disclose an individual’s protected health information when required to do**
239 **so by other law through a covered entity’s notice of privacy practices. Based on**
240 **comments received, we have been informed that accounting for these**
241 **nondiscretionary disclosures represents a significant administrative burden on**
242 **covered entities. Thus, we propose that disclosures made under § 164.512(a)(1) of the**
243 **Privacy Rule need not be included in an accounting in order to lessen this**
244 **administrative burden. (31433)**

245
246 HIMSS supports the proposal as identified by OCR. HIMSS requests clarification as to
247 whether disclosures that are executed by access to an electronic DRS are required to be
248 represented in the Access Report and whether there are any exceptions (e.g. for reports of
249 victims of abuse), as this is not clear in the NPRM.

250
251 8. **[OCR requests] comment on whether a shorter 30-day deadline, with a single 30-day**
252 **extension, will significantly benefit individuals and whether it will place an**
253 **unreasonable burden on covered entities. (31435)**

254
255 HIMSS appreciates the opportunity to comment. Coordinating information between and
256 among CE and BAs could be difficult given these timeframes. Many healthcare
257 organizations have hundreds of BAs. HIMSS therefore feels that the initial 30 day deadline
258 may be difficult for organizations to meet. The amount of time required could be even
259 greater than contemplated under the NPRM if the DRS definition applies. The amount of
260 data and systems involved could increase exponentially in cases where multiple CEs and
261 BAs must access, log, and collate relevant databases. It is highly unlikely that current
262 systems will be able to adequately respond within a 30 day period. Until this issue is
263 studied, more, not less time, may be the better course of action.

264
265 Finally, a significant factor in commenting on whether this deadline with an extension
266 option is viable is the process for requesting an extension. As the process for requesting an
267 extension is not specified in the NPRM, it is difficult to assess this requirement in its
268 totality. However, HIMSS feels that the extension process should not create an overly
269 cumbersome administrative burden to healthcare organizations, and the request should be
270 processed in a timely fashion.

271

272 9. **To the extent that the covered entity is able to provide more information, such as a**
273 **description of the system that is accessing the information, we encourage covered**
274 **entities to include such information. We recognize that more information than the**
275 **covered entity’s name would be helpful to the individual, but we have concerns about**
276 **the burden on covered entities if they were to have to describe each internal exchange**
277 **of information between systems in more detail. In contrast, we believe individuals’**
278 **interest in such internal exchanges may be limited. We request comment on this issue,**
279 **particularly the burden of providing identifying information about internal systems**
280 **and the interests of individuals in learning of such internal exchanges. (31438)**
281

282 HIMSS is concerned that the described approach would be excessively burdensome if an
283 organization is using multiple IT systems as it relates to the Designated Record Set.
284

285 10. **While we recognize that it may be helpful to individuals to learn what information**
286 **was accessed, we believe that it would be unreasonable to require all covered entities**
287 **and business associates to modify all of their electronic designated record set systems**
288 **to collect this information, especially in light of the relatively small number of**
289 **accounting requests that most covered entities have received to date. We request**
290 **comment on the availability of this information in current access logs, the importance**
291 **of the information to individuals, and the potential administrative burden of**
292 **requiring that access reports include a description of what information was accessed.**
293 **(31438).**
294

295 HIMSS appreciates the question. For many EHR systems (particularly certified EHRs)
296 audit logs may contain some characterization of the type of information. In these cases,
297 HIMSS suggests utilizing the EHRs to collect the data, as it would create the least amount
298 of disruption to existing processes and the least amount of administrative burden for the
299 provider. In the event that the data is stored in an alternate IT system, HIMSS suggests the
300 final rule should require that a characterization of the data accessed should appear in the
301 Access Report if the electronic system is capable of collecting this information during the
302 course of access
303

304 11. **[OCR requests] comment on the potential burden to covered entities and potential**
305 **benefit to individuals of requiring the access report to include address information**
306 **that indicates where the access occurred. (31438)**

307 HIMSS concurs with the NPRM assertion that the address of the access location will rarely
308 be of interest and is difficult to capture. EHR certification standards may require the
309 collection of the “place” of access, but “place” is often interpreted to mean “system,”
310 “module,” IP Address, workstation ID, etc. The argument that most access happens in the
311 facility is one that gets weaker as large, multi-facility health systems service those facilities
312 from single integrated electronic systems.
313

314 12. **[OCR requests] comment on our proposal to not require covered entities and business**
315 **associates to include a description of the purpose of access in access reports. (31439)**
316

317 HIMSS appreciates the opportunity to comment on this important issue. Such information
318 is not something that is currently captured and, if required, would likely require additional
319 (and perhaps manual) data entry at the point of the action, creating an undue burden on
320 healthcare organizations.

321
322 13. **[OCR requests] comment on our assumption that systems do not record information**
323 **about the purpose of the access and ultimate recipient of the information within audit**
324 **logs. (31439)**

325
326 HIMSS agrees with this assumption. It is uncommon for systems to record the purpose of
327 the access, though purpose can frequently be inferred from the character of sequences of
328 access (e.g. a sequence that signifies a patient admission). In either case, this would be
329 extremely burdensome to CEs and BAs and therefore HIMSS supports its exclusion from
330 the reports.

331
332 14. **[OCR requests] comment on ways in which such accesses, if excepted from the access**
333 **report, could be identified and excluded in an automated way. (31439)**

334
335 HIMSS appreciates the opportunity to review the topic, and suggests OCR consider
336 allowing CEs/BAs to exclude accesses that relate to a limited set of purposes mentioned
337 elsewhere (e.g. reporting victims of abuse). This approach will prevent cases where a
338 report recipient may reasonably infer the purpose of the access.

339
340 15. **There may be significant burden in aggregating this data into a single access report.**
341 **However, we believe that this administrative burden is reasonable in light of the**
342 **interests of individuals in learning who has accessed their protected health**
343 **information. Additionally, the burden of generating access reports will be directly**
344 **proportionate to the interests of individuals; if few individuals request access reports,**
345 **then covered entities will rarely need to undertake the burden of generating an access**
346 **report. We request comment on the above conclusions. (31439)**

347
348 HIMSS is concerned that the NPRM, in particular the new right to an Access Report, fails
349 to fully reflect a balancing of the interests of individuals in learning the circumstances in
350 which their protected health information is used/disclosed against the administrative burden
351 placed on CEs and BAs as required by Section 13404 (e) (2) of the HITECH Act. HIMSS
352 suggests that the new NPRM requirements related to Access Reports may impose more
353 significant burdens than are appreciated by the government.

354
355 In addition, as currently written, the NPRM implies that OCR has assumed that the Access
356 Report requirement places a “reasonable burden” on organizations, yet offers no evidence
357 that it has collected data and conducted an analysis of the burden of this new requirement.
358 Compliance with the Access Report requirement will require sophisticated electronic
359 technology to track relevant information technology that is unavailable (on some systems)
360 or too expensive for CEs and BAs to obtain, particularly given the fact that disclosures for
361 treatment, payment and health care operations constitute the vast majority of routine
362 disclosures of protected health information by CEs and BAs. This problem is exacerbated

363 by the fact that, for most CEs and BAs, Designated Record Sets are maintained in
364 electronic form in a variety of systems, not simply in an electronic health record as was
365 contemplated by the HITECH Act, necessitating burdensome access to, logging and
366 collation of information maintained in a variety of systems. Many of these systems simply
367 do not have the capability to collect audit information in this way. Even if each system
368 could collect this information in an audit log, the Access Report requirement also would
369 require log aggregation and analysis functions that currently do not exist in most
370 organizations.

371
372 HIMSS suggests that it is not clear whether benefit to the receiving individual has been
373 properly reviewed, and requests OCR provide clarification on the following items:

- 374 • The ability of an organization to electronically track whether a person received
375 the information in a manner not reflected in the audit log.
- 376 • The lack of electronic log information in situations where consumer asks someone
377 to access the record and present a hard or electronic copy to the consumer.
- 378 • The questionable utility derived from the individual knowing the names and time
379 of such accesses.
- 380 • The uncertainty about the impact on health outcomes derived from an individual
381 knowing who viewed the record
- 382 • The lack of understanding on whether access report information helps individuals
383 navigate the delivery system more effectively.

384
385 HIMSS is also concerned that the NPRM does not recognize that Access Reports will be
386 voluminous and difficult to read and interpret by the patient. As well, it may actually result
387 in patient-initiated privacy investigations, a potential unintended consequence that was
388 likely not OCR's intent. If the patient simply requests an Access Report and does not share
389 their concerns/suspicions with the CE, this could prevent the CE from conducting privacy
390 investigations and/or administering any warranted sanctions.

391
392 With respect to the number of patient requests and the related impact of the Access report
393 process on healthcare organizations, it is clear that in order to meet the 30 day deadline,
394 organizations will have to implement the logging function on all relevant systems, and put
395 automated processes/systems into place to collate and analyze the data *ahead* of any
396 request by a patient. That is, they will have to incur all of these expenses and administrative
397 burdens a priori in order to be prepared for the first request. So, the first requested report
398 will cost (for example) \$10,000 and the second and subsequent reports will cost \$10,000
399 plus \$.02. This is another area in which the NPRM has made an incorrect assumption
400 regarding the burden on organizations.

401
402 HIMSS wishes to point out that the Secretary has authority to promulgate regulations to
403 define what information shall be collected about each disclosure. Importantly, this also
404 means that the Secretary has authority to require *no* specific or particular information about
405 any particular category of uses or disclosures. For example, if there is a category of
406 information that is of limited interest and/or greater burden, it may be possible to account
407 for this category by providing a general explanation of disclosures in that area without
accounting for each specific individual access, dates or times. Nothing in paragraph

408 13405(c)(1) appears to restrict such flexibility. A contrary reading would essentially read
409 paragraph 13405(c)(2) into a null set of data. More than just providing this *authority*,
410 Congress has applied a *burden* on HHS with respect to any new requirement: “Such
411 regulations shall only require such information to be collected through an electronic health
412 record in a manner that takes into account the interests of the individuals in learning the
413 circumstances under which their protected health information is being disclosed and takes
414 into account the administrative burden of accounting for such disclosures.”

415 Further, in assuming and using its general authority under HIPAA with respect to the two
416 Security Rule requirements mentioned, HIMSS is concerned that OCR’s presumptions may
417 not reflect common occurrences in the healthcare community, for example:
418

- 419 • The HIPAA Security Rule applies to healthcare organizations and provides
420 requirements for the organization’s efforts to protect the data that it holds. The HIPAA
421 Security Rule was never intended to impose a requirement to provide data from a
422 security audit log to patients. The point of the audit requirement is to allow the
423 organization to log information that will facilitate its own security risk management
424 process/program. The information that is logged is determined by the organization
425 itself, based on its needs. A security audit log, as implemented and reviewed as part of
426 the two requirements mentioned, typically contains data on *security anomalies* and
427 often does not log legitimate accesses, in particular “read” accesses. However, the
428 discussion in the NPRM assumes that “use” data, including data about legitimate,
429 routine read accesses, is captured in a security audit log. The NPRM, therefore,
430 imposes a *specific standard* for data collection in this log, specifically a type of data not
431 anticipated by the Security Rule.
- 432 • The NPRM seems to assume that there is a requirement in the Security Rule for
433 organizations to collect and log data on uses of ePHI. HIMSS suggests currently there
434 is no requirement in the Security Rule for an organization to actually collect this data.
435 Perhaps OCR was thinking about the requirement in the EHR Certification program
436 that requires EHRs to have the capability/functionality to facilitate the collect of “use”
437 data – the functionality to provide an access log, if desired.
438

439 On another point, HIMSS notes that there is significant healthcare community concern
440 about providing the names of individual employees to patients in the Access Report, when
441 those employees are merely performing their job duties. This requirement could
442 conceivably create personal risk to the individual employee and it is not clear that this risk,
443 nor any means to mitigate it, have been considered.
444

445 Given all of these issues, the burden of providing an Access Report as required by the
446 NPRM has not been balanced by the benefit to individuals. Treatment, payment and health
447 care operations uses and disclosures are routine and recurring and are unlikely to be of as
448 much interest to individuals as the non-routine disclosures covered under the original
449 HIPAA Accounting of Disclosures. In fact, as the NPRM notes repeatedly, in general,
450 individuals have shown little interest in exercising their right to an Accounting of
451 Disclosures in the nearly ten years since that right was conferred by the HIPAA privacy
452 rule.

453
454 HIMSS recommends that the Final Rule allow CEs and BAs to satisfy the requirements of
455 the Accounting of Disclosures for TPO statute by requiring an organization to provide an
456 individual with a written summary description of typical, relevant categories of disclosures
457 from EHRs made in the normal course of treatment, payment and health care operations,
458 since most are recurring for a given period of care. HIMSS suggests that such a summary
459 would satisfy the needs of individuals for this information in a practical and reasonable
460 way. Any additional information desired by the patient can be requested through the
461 process of a privacy investigation that can be requested by the individual and conducted by
462 the organization.

463
464 16. **[OCR proposes] to provide that machine readable data is digital information stored in**
465 **a standard format enabling the information to be processed and analyzed by**
466 **computer. For example, this would include providing the access report in the format**
467 **of MS Word or Excel, text, HTML, or text-based PDF, among other formats. We**
468 **request comment on the ability of covered entities to provide access reports in**
469 **machine readable or other electronic formats. (31440)**

470
471 HIMSS appreciates the opportunity to comment and suggests the best approach would be
472 dependent on the standard(s) and/or format(s) identified for exchanging and processing the
473 data. For example, for PDF/text, this would be easy, and may not constitute much of a
474 burden. For other structured/machine readable formats, it would depend on standards and
475 format identified for exchanging the data as to whether this would be burdensome to an
476 individual organization.

477
478 17. **Because covered entities should already be maintaining access logs pursuant to the**
479 **Security Rule, we believe that it is reasonable to require covered entities to produce**
480 **access reports, upon request, covering access over the prior three years beginning on**
481 **the proposed January 1, 2013, and January 1, 2014, compliance dates. We request**
482 **comment on whether covered entities will be able to generate access reports covering**
483 **the preceding three years on these compliance dates. (31442)**

484
485 HIMSS appreciates the question. As discussed in item #15 above, the HIPAA Security
486 Rule applies to healthcare *organizations* and provides requirements for the organization's
487 efforts to protect the data that it holds. The HIPAA Security Rule was never intended to
488 impose a requirement to provide data from a security audit log to patients. The point of the
489 audit requirement is to allow the organization to log information that will facilitate its own
490 security risk management process/program. The information that is logged is determined
491 by the organization itself, based on its needs. As implemented and reviewed as part of the
492 two requirements mentioned, a security audit log typically contains data on *security*
493 *anomalies* and often does not log legitimate accesses, in particular "read" accesses.
494 However, the discussion in the NPRM assumes that "use" data, including data about
495 legitimate, routine read accesses, is captured in a security audit log. The NPRM, therefore,
496 imposes a *specific standard* for data collection in this log, specifically a type of data not
497 anticipated by the Security Rule.

498 The NPRM seems to assume that there is a requirement in the Security Rule for
499 organizations to maintain an access log. Perhaps OCR was thinking about the requirement
500 in the EHR Certification program that requires EHRs to have the capability/functionality to
501 facilitate the collect of “use” data – the functionality to provide an access log, if desired.
502 Again, currently there is no requirement in the Security Rule for the organization to
503 actually collect this data.

504
505 Regarding the compliance dates, as stated in our summary comments, HIMSS feels that
506 HHS would benefit from reconsidering its approach and engaging healthcare community
507 members in further dialogue about how to best means for finding a balanced rule.
508 However, we also understand that the Secretary must resolve how to include required
509 Accounting of Disclosures elements relative to treatment, payment, and healthcare
510 operations (TPO) within timelines established by HIPAA. With little discretionary time
511 left, HIMSS feels that required open dialogue necessary to remediate issues within the
512 NPRM may be difficult to achieve by the statutory deadline.

513
514 As a practical matter, if this were to be implemented exactly as contemplated in the NPRM,
515 while the systems and processes might be in place by that point, requiring that the data is in
516 the log for the previous three years does not seem possible.

517
518 18. **[OCR has] limited information on how long it takes to respond to an accounting**
519 **request under the current rule. The information that we have received has suggested**
520 **that not more than 30 days is needed to respond to an accounting request under the**
521 **current rule. Furthermore, our proposed rule will reduce the scope of information**
522 **that is subject to an accounting. Accordingly, we believe there will be little burden on**
523 **covered entities to respond to requests in 30 days, rather than 60 days. In**
524 **circumstances where more than 30 days is needed, we continue to permit a single 30-**
525 **day extension. We solicit public comment on this issue. (31444)**

526
527 HIMSS does not agree with the NPRM assumption, as stated in our answer to question #8
528 above, that “the proposed rule will reduce the scope of information that is subject to an
529 accounting.” In fact, we have concluded that the change in scope of the required
530 information from “ePHI disclosed through and EHR” to the data in the DRS and all
531 associated systems, as well as the coordination with the BA to include their data, will
532 significantly increase the burden on organizations and does not seem possible to complete
533 in 30 days.

534
535 19. **[OCR expects] that the additional burden to covered entities will consist of, in**
536 **response to a request, generating access reports for each electronic designated record**
537 **set system and aggregating this information into a single electronic access report. The**
538 **cost to covered entities to prepare an access report would be directly tied to the**
539 **number of requests. Based on the experience covered entities have reported with**
540 **requests for accountings of disclosures, we anticipate few requests for access reports.**
541 **Therefore we expect the costs to generate access reports will be minimal. We request**
542 **comment on the number of anticipated access reports, the burden of tracking access**
543 **to electronic designated record set information, including whether our proposal will**

544 **have any unintended effects by requiring significant changes to existing systems, and**
545 **the burden caused by generating an access report. (31444)**
546

547 HIMSS appreciates the question, and suggests the cost and burden related to the new
548 Access Report requirement is not related to the number of actual requests for such a report
549 because, as discussed in #15 above, organizations do not currently typically collect data for
550 an access log in their security audit log (which is incorrectly assumed in the NPRM).
551 Therefore, as also discussed in #15 above, the organization must implement the technical
552 and administrative requirements and incur the costs prior to the first request. This is
553 excessively burdensome to an organization and may not be balanced by the benefit to the
554 patient.
555

556 20. **The provision permitting individuals to limit their requests to a time period or person**
557 **may limit the burden to produce an access report. Yet, modifying a standard report**
558 **may require additional programming which would increase burden on the covered**
559 **entity and business associates. We solicit comment on the effects of this provision.**
560 **(31445)**
561

562 HIMSS appreciates the question, and suggests the cost and burden related to the new
563 Access Report requirement is not related to any limitations by the patient on the scope of
564 such a report because, as discussed in #15 above, organizations do not currently typically
565 collect data for an access log in their security audit log. Therefore, as also discussed in #18
566 above, the organization must implement the technical and administrative requirements and
567 incur the costs prior to the first request, limited or not. This is excessively burdensome to
568 an organization and may not be balanced by the benefit to the patient.
569

570 21. **Therefore, the total cost for providers is approximately \$20 million. Because of the**
571 **uncertainty surrounding the costs for revising privacy notices, we invite public**
572 **comment on our analysis. (31446)**
573

574 This information is difficult to calculate, as the requirement is new. This topic is an
575 example of the dialogue we reference in above comments.
576

577 **Although there may be costs associated with notifying enrollees of the change to the**
578 **notice, we believe the cost should be minimal based on health plans including such**
579 **notification in their annual plan update notices. We request public comment on our**
580 **assumptions and analysis. (31446)**
581

582 This information is difficult to calculate, as the requirement is new. This topic is an
583 example of the dialogue we reference in above comments.
584

585 22. **Based on the relatively small cost per covered entity, the Secretary certifies that the**
586 **proposed rule would not have a significant impact on a substantial number of small**
587 **entities. However, because we are not certain of all the costs this rule may impose or**
588 **the exact number of small health insurers or third party administrators, we welcome**
589 **comments that may further inform our analysis. (31446)**

590
591 The assessment in the response provided by HIMSS to item #18 above applies equally to
592 small providers and therefore HIMSS feels that this NPRM will be excessively burdensome
593 for small entities. In fact, it may be disproportionately more burdensome for smaller
594 providers in that they would probably have to contract with outside consultants to assemble
595 the information in that they would not have the internal expertise to do it. For example,
596 they may need to hire a consultant to work with their EHR vendor, lab vendor, radiology
597 and other BAs in order to assemble the required report.

598
599
600 **Conclusion:**
601 HIMSS appreciates the opportunity to provide public comments to the Office of Civil Rights on
602 this important Notice of Proposed Rule Making. We look forward to continued dialogue
603 between HIMSS members and the Department, in order to achieve the benefits of the HITECH
604 Act. If you have any additional questions please contact Lisa Gallagher, Senior Director, Privacy
605 and Security, 703.562.8816; or Thomas M. Leary, Senior Director, Federal Affairs,
606 703.562.8814.

607
608 Sincerely,
609



610 | Charlene S. Underwood, MBA, FHIMSS
611 | Chair, HIMSS Board of Directors
612 | Senior Director, Government and Industry Affairs
613 | Siemens Healthcare
614
615



H. Stephen Lieber, CAE
President/CEO
HIMSS