American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

August 1, 2011

SUBMITTED VIA E-FILE

The Honorable Kathleen Sebelius
Secretary
U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, S.W.
Washington, DC 20201

Attention: HIPAA Privacy Rule Accounting of Disclosures (RIN 0991-AB62); Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (May 31, 2011).

Dear Secretary Sebelius:

On behalf of our more than 5,000 member hospitals, health systems and other health care organizations, and our 42,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to comment on the Department of Health and Human Services (HHS) Office for Civil Rights' (OCR) May 31 proposed rule on the HIPAA Privacy Rule Accounting of Disclosures under the *Health Information Technology for Economic and Clinical Health Act* (HITECH). This rule proposes changes to the HIPAA Privacy Rule for hospitals and other HIPAA-covered entities, and their business associates, affecting the individual right to an accounting of disclosures. Unfortunately, the AHA believes that the centerpiece of the proposed rule is misguided because it does not appropriately balance the relevant privacy interests of individuals with the substantial burdens on covered entities, including hospitals. As such, it is out of step with President Barack Obama's call in the January 18, 2011, Executive Order 13563, "Improving Regulation and Regulatory Review," for "cutting down on the paperwork that saddles businesses with huge administrative costs."

America's hospitals are dedicated to safeguarding the privacy of their patients' medical information, and the AHA and its members support HHS's efforts to implement HITECH's change to HIPAA. We generally endorse the proposed revisions to the accounting of disclosures requirements, although we urge additional changes to ensure that patients continue to receive information they value for understanding how their protected health information (PHI) is used and disclosed without placing undue burdens on covered entities to provide that information. However, the proposed rule's requirement for providing individuals with an access report

detailing all internal access to electronic designated record sets is misguided, as explained above; and we urge HHS to withdraw its proposal to create a new individual right to an access report.

Summarized below are additional recommendations, which we discuss in greater detail in the attached pages:

- While the AHA generally supports HHS's efforts to implement changes to the existing accounting of disclosures requirements, we request that HHS clarify the discussion of designated record sets, adopt its proposed exclusions to the accounting requirement and maintain existing exclusions. We urge HHS to maintain a 60-day response requirement and limit an accounting to three years.
- Instead of moving forward to establish the new individual right to an access report, HHS should reissue a request for information aimed at better reflecting the statutory requirements, the technological realities, and better alignment of the regulation's effectiveness with the compliance burdens.
- The AHA is concerned about the assumptions HHS makes regarding the HIPAA Security Rule in its preamble commentary and asks HHS to retract the preamble discussion in order to reflect longstanding department guidance.
- In the event HHS declines our request to abandon the access report, we urge HHS to adopt a number of changes, including extending the compliance date and removing the requirement to name employees. We also request that HHS reflect the statutory requirement that covered entities be permitted to direct individuals to a business associate. In addition, we ask that HHS make clear that a covered entity is not liable for unsecure transmissions requested by a patient. Finally, we request that HHS provide at least 60 days for the provision of an access report.

We believe that HHS can further improve the value of the rule for both patients and providers by withdrawing the proposed access report requirement and making the additional improvements we recommend. If you have any questions about our recommendations, please contact Lawrence Hughes, assistant general counsel, at lhughes@aha.org or (202) 626-2346.

Sincerely,

/s/

Rick Pollack
Executive Vice President

AHA Detailed Comments on Proposed Changes to HIPAA Regulations

ACCOUNTING OF DISCLOSURES

Clarify that an Accounting Applies Only to Information Contained in Designated Record Sets

HHS recommends amending § 164.528(a)(1) to limit the accounting of disclosures right to information contained in a designated record set. The AHA supports this proposed revision, as it is consistent with the other individual rights set forth in the Privacy Rule. However, we urge HHS to clarify its preamble language regarding designated record sets. **In particular, we request that HHS make clear that this individual right applies only when the information is contained in a designated record set and <u>not</u> to copies of the information that exists in other record sets.**

For example, hospitals often contract with state hospital associations or other private entities to carry out quality improvement activities as "business associates." These business associates may have copies of designated record sets or copies of information that are part of a designated record set when held by the hospital. When held by the business associate, however, this information is not used to make decisions about individuals; while the information held by the business associate may contain PHI that duplicates, at least in part, the PHI in the hospital's designated record set, the business associate records are not "the medical records and billing records about individuals maintained by or for a covered health care provider" as described in the definition of "designated record set" in § 164.501. This copy of the information is not used by either the business associate or the hospital to make decisions about an individual patient, but instead to run quality analyses for the hospital.

HHS's longstanding position has been that, even though PHI in a designated record set may be duplicated in other information systems maintained by the covered entity, those other systems are not necessarily designated record sets. More specifically, HHS guidance in 65 *Fed. Reg.* 82462, 82554 (Dec. 28, 2000) provides, "[c]overed entities often incorporate the same protected health information into a variety of different data systems, not all of which will be utilized to make decisions about individuals. *In that case, the information would not fall within the definition of designated record set*." In the preamble to this proposed rule, 76 *Fed. Reg*. at 31430, HHS reiterates this approach, stating that "[a]n example of PHI that may fall outside the designated record set is a hospital's peer review files. If these files are only used to improve patient care at the hospital, and not to make decisions about individuals, then they are not part of the hospital's designated record set." We urge HHS to clarify this approach in the final rule,

making clear that the accounting of disclosures requirement applies only to information when contained in a designated record set.

EXCLUSIONS TO THE ACCOUNTING OF DISCLOSURES REQUIREMENTS

All of the exclusions identified below preserve the value of the accounting of disclosures right for individuals, while limiting the burdens to covered entities. We urge HHS to adopt each of these proposed exclusions in the final rule.

Excluding Impermissible Disclosures Where a Covered Entity has Provided a Breach Notification

The AHA appreciates HHS's proposal in § 164.528(a)(1)(A) that the accounting requirements not include disclosures for which a covered entity already has informed the individual of the impermissible disclosure in a required breach notification letter. Where a covered entity has provided notification to an individual in accordance with current federal breach notification requirements, including information about the same impermissible disclosure in an accounting may be confusing to the individual. Moreover, we believe that it is not necessary to provide an accounting of disclosures about which the individual already is aware, and we recommend that the accounting requirement not duplicate information patients already have. Implementation of this approach in the final rule will avoid unnecessary confusion for patients while eliminating an unnecessary disclosure for covered entities.

Excluding Disclosures to Report Child Abuse or Neglect

The AHA supports HHS's proposal in § 164.528(a)(1)(B) to exclude from the accounting requirements disclosures made to report child abuse or neglect. We also support the agency's commentary proposing to exclude disclosures related to reports of adult abuse, neglect or domestic violence.

Proposal to Include Military and Veterans' Activities, Department of State Medical Suitability Determinations, Government Programs Providing Public Benefits

Again, we urge HHS not to require covered entities to account for disclosures about which the individual is likely to be aware or in which the individual is directly involved. Such an approach is consistent with the underlying goals of the accounting of disclosures requirements. In particular, the disclosures set forth in § 164.512(k)(1)(i) are only permitted where the appropriate military command authority has posted a public notice in the *Federal Register* of the purposes for which the PHI may be used or disclosed. Thus, there already is notice about the potential disclosure.

The disclosures set forth in 164.512(k)(1)(ii) allow military covered entities to disclose an individual's information to the Department of Veterans' Affairs (VA) upon an individual's discharge for purposes of determining eligibility for VA programs. These again would appear to be disclosures about which an individual would likely already be aware; thus it is not necessary to impose upon a covered entity to account for such a disclosure. Similarly, medical suitability determinations by the Department of State overwhelmingly appear to be disclosures about which an individual is likely to be aware and, in many cases, where an individual would have been part of the process prompting the disclosure. The AHA urges HHS to avoid requiring an accounting in these and other circumstances in which an individual is likely to already be aware of the disclosure.

Excluding from an Accounting those Disclosures Required by Law

The AHA supports HHS's proposal to exclude disclosures required by law from an accounting provided to an individual. As HHS points out in the preamble, these disclosures do not typically relate to a specific individual, rather they tend to be population based, reflecting governmental policy decisions rather than the decisions of a covered entity. Individuals are informed of these disclosures through a covered entity's notice of privacy practices. Including these disclosures in an accounting would place an additional unnecessary administrative burden on covered entities. We also agree with HHS's proposed clarification in § 164.528(a)(1)(ii) that most disclosures that would otherwise need to be included in an accounting under § 164.528(a)(1)(ii) do not need to be included in an accounting if they are required by law. We believe that HHS's proposed treatment of disclosures required by law properly balances the privacy interests of individuals with the administrative burdens imposed on covered entities and business associates that need to be able to efficiently compile and produce the accounting of disclosures.

Exclusion of Research Disclosures from an Accounting

The AHA urges HHS to adopt its proposal to exclude research disclosures from an accounting. These disclosures are made where an institutional review board (IRB) or privacy board has made a determination that the privacy interests of individuals are properly taken into consideration. While the AHA appreciates HHS's current simplified approach to an accounting of research disclosures, which allows a covered entity to provide individuals with a list of research protocols for larger studies, we agree with the concerns expressed in the preamble that the accounting requirements may deter important research. The AHA supports HHS's efforts more generally to re-examine the Privacy Rule requirements related to research, and we urge HHS to continue to consider ways to implement requirements in a manner that minimizes the burden on covered entities engaged in research. The AHA urges HHS to remove from the accounting requirement disclosures for research under 164.512(i).

Exclusion of Disclosures for Health Oversight Activities

The AHA supports HHS's proposal to exclude disclosures made for health oversight activities under § 164.521(d) from an accounting of disclosures. Much like disclosures that are required by law, disclosures for health oversight activities are almost always population based and are frequently triggered by a specific event. These disclosures focus more on covered entity activities than on any specific individual. Further, these disclosures are required by law, so it is logical that they be excluded from an accounting just as disclosures required by law are excluded. We believe HHS's assumption set forth in *76 Fed. Reg. at 31433* is correct – that "the potential burden on a covered entity or business associate to account for what may be voluminous disclosures of records is balanced by what is likely not a strong interest on the part of individuals to learn of such disclosures" – and we support HHS's proposal to exclude these disclosures from an accounting.

Exclusion of Certain Disclosures about Decedents

We support excluding certain disclosures about decedents from the accounting requirement. Specifically, we support HHS's proposal to exclude disclosures about decedents made to coroners, medical examiners and funeral directors, as well as disclosures for purposes of cadaveric organ, eye or tissue donation. These changes are consistent with HHS's other proposed changes in the broader HITECH proposed rule, *75 Fed. Reg. 40868*, with respect to information on decedents and will make it easier for hospitals to handle necessary disclosures of information following deaths without adding to the accounting of disclosures burdens.

CONTINUED EXCLUSIONS FROM THE ACCOUNTING OF DISCLOSURES REQUIREMENT

The AHA supports HHS's proposal to continue to exclude from the accounting obligation disclosures:

- To individuals of their own PHI;
- Incident to an otherwise permitted or required disclosure;
- Pursuant to an individual's authorization;
- For the facility directory or to persons involved in the individual's care or other notification purposes;
- For national security or intelligence purposes;
- To correctional institutions o in law enforcement custodial situations;
- As part of a limited data set; and
- Occurring prior to the compliance date for the covered entity.

These exclusions are consistent with maintaining a balance between individual privacy interests and the burden on covered entities in implementing the privacy requirements. These exclusions also are appropriate given the legal circumstances of the exclusions (i.e., national security purposes), with the concept that an accounting should not be required where an individual likely is aware of the disclosure (i.e., disclosures pursuant to an authorization), or that would unduly impede health care activities (i.e., disclosures incident to a permissible disclosure). The AHA urges HHS to continue to exclude these disclosures from the accounting requirement.

Maintain 60 Days as the Timeframe for the Provision of an Accounting of Disclosures

Even if revised in accordance with the suggestions above, the accounting of disclosures requirements would continue to impose significant burdens for covered entities. In our members' experience, few individuals use or value this individual right, yet each request requires a significant investment of staff time and resources. Even if the revised requirement, in the context of HHS's proposed education campaign about individual privacy rights, does not increase the frequency of requests to hospitals, the workload to ascertain and include in an accounting all appropriate disclosures will continue to be challenging for hospitals.

Consequently, the AHA is very concerned that HHS's proposal to shorten the time period for covered entities to respond to an individual request from 60 days to 30 days only adds to the burdens covered entities face in complying with the accounting requirement, without providing a meaningful enhancement to individual privacy rights. The AHA strongly requests that HHS maintain the current 60-day requirement.

Reducing the Timeframe for an Accounting to Three Years

We support HHS's proposal in § 164.528(a)(1) to limit the accounting requirements to three years. We believe this will limit the burdens on covered entities without meaningfully limiting individual privacy interests, providing an appropriate balance of the burdens and benefits.

PROPOSED ACCESS REPORT

HHS Should Withdraw its Proposal for a New Individual Right to an Access Report

The AHA believes that the proposal to create a new individual right to an access report is misguided and does not appropriately balance the relevant privacy interests of individuals with the burdens that will be imposed on covered entities, including hospitals. The proposal is based on a fundamental misunderstanding of the value to individuals of receiving the particular information that the access report would capture, as well as a misunderstanding about the

capabilities of technologies available to and used by covered entities. We believe that HHS should significantly alter its approach to ensure that any final regulatory requirements appropriately fulfill the needs of patients who seek to understand how their PHI is disclosed, while simultaneously ensuring that covered entities are technically capable of providing such information without incurring unreasonable burdens to do so. We recommend that HHS reissue a request for information aimed at bringing the regulations in line with the statutory intent and more appropriately reflecting the goal of making regulations effective while not imposing undue or unnecessary burdens on affected entities.

The administrative burden that would be imposed on hospitals and other covered entities as the result of the implementation of the proposed access report is inconsistent with the Department's other initiatives to reduce unnecessary administrative costs in the health care system. As part of health reform, for example, Congress enacted changes to the administrative simplification requirements under HIPAA, aimed at increasing the efficiency of electronic transactions and reducing associated costs. The meaningful use incentive program is designed to encourage widespread adoption of electronic health records, widely touted as a means to reduce unnecessary administrative costs in the health care system. At the same time, HHS has issued a *Preliminary Plan for Retrospective Review of Existing Rules* aimed at reducing unnecessary regulatory burden in accordance with the President's Executive Order to "promote retrospective analysis of rules that may be outmoded, ineffective, insufficient, or excessively burdensome, and to modify, streamline, expand, or repeal them in accordance with what has been learned." The AHA believes this proposed rule is incompatible with these efforts.

Scope of Access Report Should be Limited to an Accounting of PHI Maintained in EHRs

Section 13405(c)(1) of the HITECH Act provides that covered entities who maintain an electronic health record (EHR) with respect to protected health information of an individual shall provide an accounting id disclosures for treatment, payment and health care operations purposes. The AHA is concerned by HHS's proposal to expand this right to an expended accounting so that it would apply to all protected health information maintained in one or more designated record sets electronically. For covered entity health care providers, a designated record set includes both treatment and billing records maintained by the provider. For many hospitals these records are maintained across several different systems (both electronic and paper). In order to comply with a request for an access report for PHI maintained in a designated record set electronically, it would require manual identification and compilation of relevant records from each system. Many electronic systems that qualify as part of designated record set, such as billing systems, may not have the required functionality to allow them to easily download access to one patient's information. Therefore, in practice, hospitals may have to resort to printing records from such systems and then manually compiling them to provide a comprehensive report of access to PHI in electronic designated record sets.

This exercise of authority by HHS exceeds the statutory directive and disregards congressional intent. In the legislative history of the HITECH Act related to the expanded privacy rights for individuals, the House Committee on Ways and Means cited "[g]reater use of electronic health records and other forms of health IT [which] presents an opportunity to enhance transparency and accountability within the health care system in terms of how information is used" as rationale for expanded privacy requirements. We encourage HHS to modify its proposal and instead adhere to congressional intent to afford individuals a right to an expanded accounting of disclosures of PHI for treatment, payment and health care operations only if that PHI is maintained in an EHR. To do otherwise would be too onerous for covered entities.

In attempting to combine the HITECH requirement and the department's general statutory authority, HHS has come up with something that simply is not practical or even feasible for the health care system. This approach fails to acknowledge the profound burden imposed on covered entities, while at the same time failing to achieve a stated privacy goal. It does not balance burden and benefit. The AHA strongly urges HHS to reissue a request for information, and to work with stakeholders to devise a solution that reflects the statutory intent and balances an identifiable privacy interest with the costs of implementing additional complex requirements.

HHS Should Withdraw its Preamble Statements on the Security Rule

HHS's proposal for an access report is based in an entirely new reading of the Security Rule. The preamble language describing the Security Rule is inconsistent with HHS's guidance to covered entities over time, and we ask that HHS retract this preamble discussion so as not to create confusion for covered entities and business associates attempting to comply with the Security Rule. Most significantly, HHS presumes that the Security Rule requires an audit log that captures the information that HHS proposes to require in an access report. From the outset, HHS has established an approach to Security Rule compliance that is flexible, scalable and technology neutral. The Security Rule specifically states in § 164.306(b) that covered entities "may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." HHS has repeatedly reiterated this approach in related guidance. Yet in the proposed rule, HHS suggests that entities in compliance with the Security Rule will be able to easily incorporate the requirements of the access report, based on audit log activity. Yet the Security Rule does not require the types of audit logs that HHS contemplates in this proposed rule. Rather, one of the Security Rule's technical safeguards standards is that a covered entity should have "audit controls." The regulation states in § 164.312(b) that this means the implementation of "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." In providing guidance on this standard, at *68 Fed. Reg. 8355*, HHS stated that it "support[s] the use of a risk assessment and risk analysis to determine how intensive any audit control function should be." HHS has <u>not</u> required this audit log to capture the type of information proposed in the access

report. Indeed, HHS acknowledges that even its own rules for certified health records do not contain this capability. The AHA requests that HHS withdraw its preamble discussion regarding the Security Rule and instead revert to its longstanding guidance about the Security Rule generally and audit logs in particular.

The Changes Contemplated by the Access Report Ignore Substantial Burdens for Covered Entities

As discussed above, the proposal for an access report arises out of a misguided interpretation of the Security Rule; rather, in order to come into compliance with the access report proposal, covered entities would need to make substantial changes to their IT systems. We are concerned that HHS's proposal for an access report ignores the real burdens to covered entities related to these changes. Capturing the scope of information proposed and processing audit trail information into a form that is reasonable and understandable by a patient will be a major undertaking. The processing time for an information system to generate audit trail information can be significant. Moreover, there are potentially significant costs involved in storing audit trail data in the manner HHS suggests.

In assessing the burden to covered entities, HHS fails to take into account that electronic systems currently do not have the technical capability to generate an access report that is meaningful to, and understandable by, a patient and that can be handed over to a patient without significant work. Indeed, even certified EHR systems operating consistent with the meaningful use requirements are not capable of generating an audit report that can be translated into an access report in the manner that HHS contemplates. Certainly, if HHS's own requirements related to certified EHRs cannot accomplish this, it is clear that older electronic systems are not likely to have audit log processes that can be readily transformed into an access report. Generating an access report involves a complex and time-consuming process to analyze large volumes of data; this currently cannot be accomplished without human intervention. Vendors of these systems are not required to provide this capability, and it typically has not been included in system design. Some vendor estimates suggest that the costs of an audit capability for systems that would generate information to facilitate an access report could be $3 million per system. For a hospital with multiple systems, it generally will not be financially feasible to upgrade all the systems in the current environment where significant expenditures are incurred to upgrade health IT systems for meaningful use and where there is increased pressure from government, insurers and patients to reduce the costs of health care delivery.

The Proposed Access Report offers Questionable Benefit to Individuals

We also question the benefit an access report will provide to patients. A recent accounting request received by a member hospital for a patient with a length of stay of 30 days generated an audit report, showing access within the hospital, of approximately 1,500 pages. This audit log

identified the screen shot that was accessed, but not the specific data accessed. Another hospital maintains audit logs for its laboratory systems, but the audit log tracks only access to the system, not access to any particular individual's PHI. Specific actions taken during an access may be difficult to identify from an audit trail, especially when the action taken is to print information. Processing time necessary to run an audit report is not insignificant – generating an audit trail report can take as long as six-eight hours per report. While this may be a necessary activity as part of ensuring a secure database, this typically is conducted on a periodic basis for a system, such as weekly or monthly. Running audit trail reports on a specific individual's PHI, where a system can even identify information in this manner, could be a substantial time commitment for covered entities.

Moreover, there are a number of ways in which patients are informed about how their information is used and disclosed by a covered entity. For example, patients receive a hospital's Notice of Privacy Practices, which includes not only a general description of the types of uses and disclosures for treatment, payment and health care operations, but also specific examples of each type of use and disclosure. Importantly, the notice also contains information about how individuals can communicate with a covered entity if they believe their information may be at risk of misuse or their privacy rights have been violated. The experiences of hospitals to date suggest that patients are more interested in knowing whether a specific violation relating to their EHR has occurred and getting detailed information in response to a specific inquiry and investigation by the hospital's privacy and compliance staff. Patients value these investigations because they provide information about specific violations and what appropriate disciplinary and other measures were taken to ensure that violations do not reoccur. A patient concerned about a future potential misuse, such as a relative working in the hospital who may inappropriately access records, also can use this mechanism to work with a hospital in advance to create a process for minimizing the possibility that such inappropriate access will occur. These processes and practices already are in place and are aimed to ensuring that patient are getting the information they feel they need and most value. It is not necessary to create an over-broad access report requirement to capture the specific issues for the few patients who have individual access concerns.

For the reasons described above, the AHA strongly recommends that HHS withdraw the access report proposal in its entirety. **If HHS elects to adopt the proposed access report despite compelling reasons not to do so, we request that HHS at least make the following changes to the access report.**

Extend the Compliance Date if the Access Report is Adopted. Should HHS choose to adopt the access report rather than withdraw it, the AHA requests that HHS make the compliance dates for the proposed access report provisions as late as possible. We believe that the current compliance dates for the access report provisions of the proposed rule, set forth in *76 Fed. Reg.* at 31442, do not give covered entities and business associates enough time to deal with the

operational changes and expenses that will be required to comply with the proposed rule. Put simply, we believe that many covered entities and business associates will not be able to comply by the proposed dates of January 1, 2013 and January 1, 2014. Since HHS has proposed requirements that are far more complicated and involved than the HITECH Act provisions, we believe that the statutory compliance dates should not apply to HHS's proposed changes. We do not think HHS should be bound by the January 1, 2013 compliance date for systems acquired after January 1, 2009 or the January 1, 2016 compliance date for systems acquired before January 1, 2009, as it is proposing a new right not derived directly from the statute.

We also urge HHS to consider the myriad other regulatory obligations that covered entities and business associates are facing when setting the compliance date for the proposed access report provisions. *The Patient Protection and Affordable Care Act's* (ACA) administrative simplification provisions, the adoption of new EHR systems to meet meaningful use, and the implementation of ICD-10 all require resources and financial investment. Given the number and scope of IT changes that covered entities and business associates will be required to undertake, both in order to comply with the proposed rule and for other competing priorities, we believe that a later compliance date is necessary.

HHS states, *76 Fed. Reg. 31442*, that "it is reasonable to require covered entities to produce access reports, upon request, covering access over the prior three years, beginning on the [proposed compliance dates]." HHS requests comments on whether compliance with this proposal would be possible. We believe that covered entities and business associates will not be able to create access reports for the three years prior to the compliance date as suggested in the proposed rule. We urge HHS to require that access reports include information accessed starting on the compliance date and going forward. As we have pointed out in this comment letter, we believe that covered entities and business associates will face difficulty complying with the proposed access report provisions going forward; complying with these provisions retroactively will be even more difficult. The primary reason for this is that much of the technological infrastructure that will be required to produce an access report does not yet exist, so tracking the information required for the access report before the proper systems are in place will be impossible.

Employees Should Not Be Named in Access Reports. The AHA believes that the access report provisions of the proposed rule raise concerns relating to the privacy and safety of hospital employees. Specifically, the proposed rule would require covered entities to produce access reports detailing the names of employees who have accessed an individual's record. This access would have to be reported even if the employee accessed this information in the ordinary course of his or her job, which will almost always be the case. The creation of an access report detailing specific covered entity employees could lead to the harassment, or even physical harm, of the employee at the hands of the individual requesting the access report.

As stated above, patient records overwhelmingly are accessed for permissible purposes. Nonetheless, if a former patient had a bad experience or outcome, the former patient may try to use the information in the access report to target hospital employees that the former patient views as responsible for the bad experience or outcome. Further, the provision of the proposed access reports might lead hospital employees to refuse to do certain jobs, as they may be fearful of being included in an access report. Protecting employee privacy must be a consideration for HHS. This protection is even more important in the health care context where employees are performing sensitive jobs where emotions can run high. We fear that the creation of the individual right to access reports will do little to enhance patient privacy while simultaneously creating a new, larger privacy problem for employees of covered entities and business associates.

Covered Entities Should Be Able to Limit Patient Choice with Respect to Electronic Format. HHS proposes at §164.528(a)(3)(ii) to require covered entities to provide an access report in a form and format requested by the individual, if it is readily producible. The AHA believes that it is reasonable for covered entities to accommodate the individual's requested format where possible but urges HHS to clarify that patients do not have unlimited choice if their preferred option is not available. We suggest that each covered entity should have the flexibility to determine the variety of electronic formats it will offer, and a patient should be required to select from those available formats if his or her preferred format is not readily producible.

The proposed rule and associated commentary is not sufficiently clear with respect to a covered entity's obligations to ensure that the protected health information remains secure during transmission when providing an access report to an individual. The AHA is aware that hospitals have an obligation to safeguard protected health information in compliance with the Security Rule. Consistent with the Security Rule, HHS states in the preamble, *76 Fed. Reg. 31435*, that covered entities are responsible for ensuring that reasonable safeguards are in place to protect the information when responding to requests for access reports. However, HHS also indicates that if an individual requests a communication in a format that is not secure, the covered entity should comply with the request. If this is the case, we ask that HHS also make clear that, where a hospital is asked to provide an individual with an access report (or an accounting of disclosures) in an electronic format that is not secure, the hospital is not liable for the information once it is transmitted.

Clarify that an Access Report Applies Only to Information Contained in Designated Record Sets. As we urged with respect to the accounting of disclosures, we urge that HHS make clear that the access report applies only to information contained in a designated record set. The AHA's previous analysis of the definition of designated record set and its application to the accounting of disclosures on page 3 of these comments applies equally with respect to the access report. We urge HHS to make in the final rule a similar clarification of the approach for the access report.

Permit Covered Entities to Direct Individuals to a Business Associate. The AHA urges HHS to adopt the HITECH language regarding an accounting of disclosures by a business associate if HHS decides to implement the access report. Under HITECH § 13405(c)(3)., covered entities are permitted to provide to an individual an accounting that includes an accounting for disclosures made by business associates. Alternatively, a covered entity may choose to provide an accounting only for those disclosures made by the covered entity, and "provide a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address." HHS has disregarded this statutory language and instead proposes to implement the access report by requiring that a covered entity include a business associate's uses and disclosures, without providing an option for a covered entity to direct an individual to the business associates. If HHS decides to adopt the access report, we urge the department to implement the statutory provisions allowing covered entities the option to direct individuals to their business associates. While HHS argues that the proposed access report is derived from the HITECH accounting of disclosures requirement, it has not incorporated these statutory requirements into the proposed rule.

Implementing this option will allow a covered entity to direct an individual to a business associate when appropriate. This is particularly important in the context of the access report. As described above, a hospital is likely to have multiple electronic systems that contain designated record sets, and these systems may not have compatible audit log capabilities, making the compilation of an access report an extremely time-consuming process. This problem is magnified when the electronic designated record sets maintained by a business associate must be included in the same access report. The need to manage the technical and manual components of compiling an access report that includes an accounting of disclosures by multiple business associates has the potential to significantly delay the provision of an access report. The AHA requests that HHS permit a covered entity to make the determination of whether to include an accounting of business associate uses and disclosures to direct individuals to its business associates. This is consistent with the choices offered a covered entity under HITECH.

Timeframe for Providing an Access Report Should Be at Least 60 Days. The AHA maintains that 60 days is necessary to make determinations about how to respond to a request no matter the format of the PHI. As described above, the process of determining which records are relevant and appropriate in response to a request for an access report and compiling access records from different systems into a readable report will be time consuming. Thirty days simply will not allow hospitals the time necessary to provide an access report.