



American  
Clinical Laboratory  
Association

## American Clinical Laboratory Association's Concerns Regarding the Privacy Provisions of the House and Senate Stimulus Packages

While clinical laboratories support efforts to improve the privacy and security of individuals' protected health information (PHI), we are concerned that new requirements under the Health Insurance Portability and Accountability Act (HIPAA) may, in fact, impose unnecessary burdens on covered entities and business associates and even compromise patient privacy. Overall, clinical laboratories, like other health care providers, have established procedures and processes to comply with the complex requirements pursuant to HIPAA. This legislation, however, will now require laboratories and other providers to develop additional procedures and processes, at a considerable expense, to address new requirements proposed by the privacy provisions included in the House and Senate Stimulus Packages. These new requirements are, in many cases, conflicting, duplicative, and unnecessary. We have highlighted below some of our key concerns with respect to these provisions.

**Notification in the Case of Breach (§ 4402(a)):** Requires that a covered entity or business associate notify each individual whose unsecured PHI has been accessed, acquired, or disclosed as a result of a breach.

- *The requirement for notification should take effect only if some level of harm results from the breach. Otherwise, covered entities and business associates would be required to notify individuals each time PHI is inadvertently misdirected although no harm results, which would be unnecessarily burdensome and costly for providers.*

**Breaches Treated as Discovered (§ 4402(c)):** A breach is treated as discovered by a covered entity or by a business associate as of the first day on which the breach is known.

- *The timeline for making such notifications should be based upon confirmation of the breach by the covered entity or business associate, as opposed to "the first day" on which the breach is known to the covered entity or business associate. This would allow the covered entity or business associate to validate that a breach has, in fact, occurred and determine whether it is necessary to notify the individual involved.*

**Requests for Restrictions on Disclosures (§ 4405(a)):** Requires covered entities to comply with requested restrictions on disclosures of PHI if such disclosures are to a health care plan for payment or health care operations and the PHI relates to health care services that the provider has been paid for by the individual out of the individual's pocket.

- *It may not be technologically feasible for laboratories to separate data for individual patients based on whether a patient has paid out of pocket because laboratories routinely make certain PHI available to plans for payment and health care operations, and in many instances the laboratory relies on patient eligibility data received from the health plan to assist in identifying whose data should go to the health plan. In addition, laboratories do not have direct patient*

*contact in most instances, and rely on the information provided by the ordering doctors, which may not properly indicate that the individual, rather than the health plan, is paying for the service.*

**Accounting of Protected Health Information Disclosures (§ 4405(c)):** Requires covered entities that use electronic health records with respect to PHI to account for disclosures relating to treatment, payment, and health care operations for 3 years prior to the date of the request. Under HIPAA, no accounting is required for treatment, payment, or health care operations, as those disclosures can be made without patient authorization.

- *The term “electronic health records” is overly broad and could include any electronic retention of a health record used in the operation of a health care provider. The term should be amended to specifically exclude information systems used for test ordering, reporting, billing and test results delivery.*
- *Given the billions of laboratory transactions each year, this requirement would be extremely burdensome, prohibitively expensive, and likely result in significant laboratory system delays.*

**Review of Health Care Operations (§ 4405(d)):** Directs the Secretary to narrow the definition of “health care operations” to exclude those activities that can reasonably and efficiently be conducted through the use of information that is de-identified or that should require a valid authorization for use or disclosure.

- *To the extent the revised definition imposes additional obligations to de-identify data that currently constitutes health care operations; it will require laboratories to conduct extensive system analysis and changes to exclude activities that will no longer be considered health care operations.*
- *This change will also impact laboratories’ abilities to conduct internal operations and to meet the needs of health plans and other entities that rely on laboratory data for secondary uses.*

**Prohibition on Sale of Electronic Health Records or Protected Health Information Obtained from Electronic Health Records (§ 4405(e)):** Prohibits the exchange of remuneration for any PHI without prior patient authorization, unless one of the enumerated exceptions is satisfied.

- *Although laboratories do not directly sell PHI, this prohibition could result in a number of unintended consequences, such as limiting the availability of certain data needed for legitimate purposes, given that PHI must be provided in the course of furnishing laboratory services.*
- *The limits on the exchange PHI could also adversely affect the effectiveness of the Nationwide Health Information Network (NHIN), as well as patient safety and quality improvement initiatives.*

**Access to Certain Information in Electronic Format (§ 4405(f)):** Requires that a covered entity provide access to PHI in an electronic format if the covered entity uses or maintains an electronic health record.

- *This provision could be interpreted to include laboratory information systems as electronic health records.*
- *Permitting individuals access to PHI electronically raises significant concerns with respect to authentication and ensuring that the information is provided to the individual requesting the information. This is particularly problematic for laboratory services because laboratories are indirect providers, often do not have a billing or face to face relationship with the patient and, thus, do not have information about the patient to authenticate their identity for the purposes of providing access – this provision could actually compromise the privacy of PHI.*
- *Covered entities would be required to establish secure systems to allow for PHI to be transmitted electronically to individuals to ensure that the HIPAA security rules are not violated.*
- *Laboratories could be required to provide individuals access to PHI, although laboratories are covered entities whose obligations related to providing access under HIPAA are subject to the limitations of applicable state laws, per the requirements under the Clinical Laboratory Improvements Amendments of 1988 (CLIA).*

**Tiered Increase in Amount of Civil Monetary Penalties (§ 4410(d)):** Establishes a tiered approach for applying civil money penalties for violations under HIPAA of \$100 to \$50,000 for each violation, and not to exceed \$25,000 to \$1,500,000 for the same violations within a calendar year, respectively.

- *These civil monetary penalties are exorbitantly higher than the penalties under existing law and fail to appropriately reflect the nature of the violation.*

**Enforcement Through State Attorneys (§ 4410(e)):** Permits Attorneys General of a State to bring a civil action on behalf of residents of the State for violations under HIPAA.

- *This provision enables an unprecedented private right of action for violations under HIPAA, which will create unnecessary lawsuits and further overload the judicial system and increase costs to taxpayers.*

\* \* \*

*We hope you find this information useful. If you have any questions, please do not hesitate to contact us.*