JONES WALKER

BANKING & FINANCIAL SERVICES

HHS' HIPAA OMNIBUS FINAL RULE: COULD THIS APPLY TO FINANCIAL INSTITUTIONS?

After much anticipation, on January 25, 2013, the Department of Health and Human Services ("HHS"), Office of Civil Rights published in the *Federal Register* the long-awaited Health Insurance Portability and Accountability Act of 1996 ("HIPAA") omnibus final rule (the "Final Rule"). Among other things, the Final Rule makes significant changes to and expands the definition of "business associate" and imposes liability on business associates and certain subcontractors of business associates for compliance with HIPAA's Security Rule and certain provisions of HIPAA's Privacy Rule (collectively, "HIPAA Rules").

Whether a bank or financial institution that performs services on behalf of a health care client is a business associate is a factual determination, which is based on an analysis of the specific facts and circumstances of each financial institution's arrangements with its health care clients. The preamble to the Final Rule provides some guidance as to when a banking or financial institution may become a business associate. The preamble first notes that, generally, the HIPAA Rules (including the business associate provisions) do not apply to banking and financial institutions "with respect to the payment processing activities identified in §1179 of the HIPAA statute,[1] for example, the activity of cashing a check or conducting a funds transfer." Section 1179 of the HIPAA statute, the preamble states, exempts certain activities of financial institutions from the HIPAA Rules, to the extent that these activities constitute authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for health care or health plan premiums. However, the preamble then notes that a banking or financial institution may be a business associate where the institution performs functions *above and beyond* the payment processing activities identified above on behalf of a Covered Entity.[2] The preamble notes that this would be the case, for example, if the banking or financial institution performs accounts receivable functions on behalf of a health care provider. Further, the preamble explains that a business associate relationship is established by virtue of the services the business associate provides and

[1] Section 1179 (42 U.S.C. §1320d–8) states in pertinent part, "To the extent that an entity is engaged in activities of a financial institution (as defined in section 1101 of the Right to Financial Privacy Act of 1978), or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for a financial institution, this part, and any standard adopted under this part, shall not apply to the entity with respect to such activities, including the following: (1) The use or disclosure of information by the entity for authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or health care, where such payment is made by any means, including a credit, debit, or other payment card, an account, check, or electronic funds transfer. (2) The request for, or the use or disclosure of, information by the entity with respect to a payment described in paragraph (1)—(A) for transferring receivables; (B) for auditing; (C) in connection with—(i) a customer dispute; or (ii) an inquiry from, or to, a customer; (D) in a communication to a customer of the entity regarding the customer's transactions, payment card, account, check, or electronic funds transfer; (E) for reporting to consumer reporting agencies; or (F) for complying with—(i) a civil or criminal subpoena; or (ii) a Federal or State law regulating the entity."

[2] "*Covered entity* means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. §160.103.

whether they involve protected health information ("PHI"),[3] and that such relationships can exist regardless of whether the parties enter into a business associate agreement or other written contract.

Of note, a broad expansion of the definition of "business associate" under the Final Rule is the inclusion of certain subcontractors of business associate into the definition. A "subcontractor" of a business associate is defined in the Final Rule as "a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate." HHS explains in the preamble that a subcontractor is a person to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for a Covered Entity (or another business associate). HHS further explains that such a subcontractor will be considered to be a business associate if the function, activity, or service involves the creation, receipt, maintenance, or transmission of PHI. Accordingly, the definition of "business associate" now includes "a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate." This means that, as described by HHS, "downstream entities" that work at the direction of or on behalf of a business associate and create, receive, maintain, or transmit PHI are now considered to be business associates themselves, and are therefore required to comply with the applicable Privacy and Security Rule provisions in the same manner as the business associate (and likewise would incur liability for acts of noncompliance). For example, if a financial institution is a business associate of a Covered Entity and hires a company to handle document shredding to securely dispose of paper and electronic PHI, then the shredding company would be a business associate of the financial institution and would be directly required to comply with the applicable requirements of the HIPAA Rules.

As discussed above, if a bank or financial institution is a business associate of a Covered Entity under HIPAA, it will have to comply with the applicable provisions of the HIPAA Rules and will be liable for its failure to do so. Compliance with these provisions will include, among other things, promptly putting in place a number of policies, procedures, and practices, entering into and/or modifying business associate agreements, and providing training on HIPAA and HIPAA compliance. In addition, if a bank or financial institution is a HIPAA business

---

[3] "*Protected health information* means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years." "*Individually identifiable health information* is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. §160.103.

associate and delegates a function, activity, or service to a "subcontractor" that involves the creation, receipt, maintenance, or transmission of PHI, then the subcontractor will also be a business associate, which will require financial institutions to, among other things, enter into agreements with the subcontractor that include specific provisions required by the HIPAA Rules. Financial institutions that are business associates, as well as any of its business associate subcontractors, have until September 23, 2013, to come into compliance with the HIPAA Final Rule.[4]

Should you have any questions regarding the foregoing, or any questions regarding HIPAA, business associates and/or business associate agreements in general, please do not hesitate to contact Lynn M. Barrett, Esq.

[4] We wish to note that the Final Rule contains a one-year transition period for implementing business associate agreements under certain circumstances.

JONES WALKER

BANKING & FINANCIAL SERVICES

Remember that these legal principles may change and vary widely in their application to specific factual circumstances. You should consult with counsel about your individual circumstances. For further information regarding these issues, contact:

Ronald A. Snider
Jones Walker LLP
254 State Street
Mobile, AL 36603
251.439.7548 tel
251.431.9401 fax
rsnider@joneswalker.com

Michael D. Waters
Jones Walker LLP
One Federal Place
1819 Fifth Avenue North, Suite 1100
Birmingham, AL 35203
205.244.5210 *tel*
205.244.5410 *fax*
mwaters@joneswalker.com

Banking & Financial Services

Ed J. Ashton
Kyle M. Bacon
Robert B. Bieck, Jr.
James L. Birchall
John C. Blackman, IV
James L. Butera
Robert L. Carothers, Jr.
Edward B. Crosland, Jr.
Donald L. Cunningham, Jr.
Allen E. Frederic, III
April Reeves Freeman
Elizabeth J. Futrell
Palmer C. Hamilton
Regina N. Hamilton
Carl C. Hanemann
Ben H. Harris, III
Arnold I Havens
Curtis R. Hearn
William H. Hines
Robert B. House
Gina M. Jacobs
John J. Jaskot
Karen B. Johns
Theodore W. Jones
Gregory W. Kuehnle
Craig N. Landrum
George A. LeMaistre, Jr.
David A. Lester
David L. Martin
R. Lewis McHenry
Katharine F. Musso
Michel Nicrosi
J. Marshall Page, III
H. Gary Pannell
R. Joseph Parkey, Jr.
Leigh Lichty Pipkin
Jeffrey T. Powell
Rudolph R. Ramelli
Kirkland E. Reid
Tyler J. Rench
Peter J. Rivas
Dionne M. Rousseau
Ralph H. Smith, II
Ronald A. Snider
Susan M. Tyler
R. Patrick Vance
Alan M. Warfield
Michael D. Waters
David S. Willenzik
Neal C. Wise
Richard A. Wright
Joshua E. Young

This message and any attachment hereto is subject to the privilege afforded Attorney Work Products and Attorney-Client communications.

JONES WALKER

BANKING & FINANCIAL SERVICES

This newsletter should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult your own attorney concerning your own situation and any specific legal questions you may have.

To subscribe to other E*Bulletins, visit http://www.joneswalker.com/ecommunications.html.