Offshore Outsourcing of Health Data Services

Your hospital is justifiably proud of its state-of-the-art Electronic Medical Record system. It hums along like a well-tuned engine, making medical errors from legendary poor physician handwriting a thing of the past. The staff has just completed its training on the Radio Frequency Identification patient bracelets, which will provide up-to-the-minute data on the patient as the physician approaches, Tablet PC or PDA in hand.

The project was, as expected, exorbitant in its cost, but the CIO saved hundreds of thousands of dollars by finding outsource providers in Pakistan for technical support, billing and claims functions, for a fraction of what these services would cost in the U.S. Yesterday, though, the CIO arrived in your office, drenched in sweat, holding a printout of an e-mail in a trembling hand. An offshore tech support provider in Pakistan has demanded a one hundred percent increase in his fee. If he does not receive an amended contract reflecting the new fee, he writes, he will post all the data, with patient identifiers, on the Internet. In his panic, the CIO called the General Counsel, in his office right away, and wants to know the Hospital’s risks and exposure if the outsource provider makes good on his threat.

The scenario above is fictional only in the most technical sense, for the trend toward outsourcing services which access personally identifiable health data is accelerating. The loss of jobs through outsourcing promises to be a hot topic in presidential debates this fall, but, as Bob Davis wrote in The Wall Street Journal, “Americans’ concerns over privacy could do more to stop overseas outsourcing of white-collar jobs than all the hand-wringing over job losses.”

The use of offshore contractors has increased dramatically in recent years due to the increased flexibility in services offered by new information technology. There has been a concomitant rise in the privacy concerns of consumers with regard to improper disclosures of personal data, and fraud such as identity theft. In the financial industry, the practice of utilizing foreign outsourcing providers is so prevalent that some journalists use the term “offshore” as a verb. The health care industry is moving toward greater use of Information Technology, particularly in the transition to Electronic Medical Record systems (“EMR”). The President’s Information Technology Advisory Committee has published a series of recommendations to advance “computerizing health records.”

The momentum of the movement toward electronic medical records and processing systems is intertwined with the upward ratcheting of concerns about protection of medical privacy. This may be expected, but the strange political bedfellows created by these issues highlights the need for vigilance among providers and plans. Following up on the President’s initiative, Senator Edward Kennedy has introduced a bill which would institute penalties by reducing reimbursements for providers who fail to adopt systems for electronic medical records and claims processing. Senator Hillary Clinton has introduced a bill which would require health care consumers to consent to the transfer of their information to offshore subcontractors in countries which have “adequate privacy protection,” and would provide for a private right of action “for any damages arising from the improper storage, duplication, sharing, or other misuse of personally identifiable information by the business enterprise or by any of its foreign affiliates . . .” The Wall Street Journal, certainly no friend of Senator Clinton during her years as First Lady said that, with regard to this bill, she was “on to something.”

The concerns of patients and health plan subscribers will increase with the movement toward computerization of medical records and increased reliance on outsourcing providers and, with them, the search for accountability for inappropriate dissemination of health data. Such services as technical support, transcription, collation, billing, insurance claims’ processing, and x-rays analysis are sent overseas with increasing frequency, as hospitals and health plans come under greater pres-
Offshore Outsourcing  Continued

sure to cut costs. It has been estimated that the twenty billion dollar industry which transcribes physicians’ dictated notes into written form sends as much as half of its work overseas. Counsel to health care providers and plans, then, must be concerned with potential liability — not to mention damage to their clients’ reputations — should one of these offshore providers disclose Protected Health Information (“PHI”).

A Cautionary Tale: UCSF

The economic benefits of outsourcing can evaporate quickly when things go awry, as the University of California at San Francisco (“UCSF”) Medical Center learned in October 2003. Like many other hospitals in the San Francisco Bay Area, UCSF outsourced transcription services, and it utilized the services of a Sausalito firm which had worked with the Medical Center for many years. The transcription firm maintained a large network of subcontractors across the country, and the use of subcontractors was known to the Medical Center. However, one of the subcontractors, a woman located in Florida, had her own network of sub-subcontractors, one of whom, in Texas, further subcontracted work to a woman in Pakistan. The Pakistani woman became angry when her fee was not paid, and her ire increased when her inquiring e-mails went unanswered.

With her own bills to pay, the Pakistani woman sought recourse through a direct e-mail to the Medical Center, containing the following threat: “Your patient records are out in the open, to be exposed, so you better track that person and make him pay my dues or otherwise I will expose all the voice files and patient records of UCSF Parnassus and Mt. Zion campuses on the Internet.” To show that her threat was credible, she attached two patient files to her unsecured e-mail. IT personnel, unsure of the source of the e-mail or whether the files were genuine, forwarded the message to the medical records department. The attached files were compared to the hospital’s records and were found to be authentic.

The Florida sub-contractor paid the woman in Pakistan, who then e-mailed the Medical Center to rescind her threat. In her message, she stated that she had destroyed the files attached to the earlier e-mail, but the Medical Center never, in fact, received evidence that the files had been destroyed.

The Medical Center has taken steps to tighten its contracts to restrict sub-contracting, but it has not discontinued the practice of outsourcing identifiable patient data. Similarly, Massachusetts General Hospital has outsourced x-ray and transcription services and, shortly after the incident with UCSF Medical Center became known, defended its agreements with a number of Indian subcontractors.

One must ask whether a contract, no matter how solid, can effectively bind offshore providers who are beyond the reach of U.S. law. Without such assurances, medical information outsourced to foreign providers can hang over the heads of hospital CIO’s, CEO’s, and counsel like a cyber-sword of Damocles, in that the repercussions to the institution if the offshore provider disseminates confidential information can be quite severe.

HIPAA

One may, at first glance, believe that this problem should have been resolved by The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Yet, HIPAA does not directly address the possibility of confidentiality malfeasance by health information subcontractors. The Department of Health and Human Services (“HHS”), the agency charged with enforcement of HIPAA, has no jurisdiction over outsourcing providers. There is no private right of action available to aggrieved health care consumers under the Privacy Rule (“the Rule”). There are, however, provisions of the Rule (though somewhat thin) under which a covered entity may be held accountable for the acts of its offshore (or domestic) vendor.

HIPAA covers only three categories of entities: health plans, clearinghouses, and health care providers who transmit data for Standard Transactions (usually billing and claims information) by electronic means. It provides that PHI may not be used or disclosed, subject to exceptions elsewhere in the Rule, except for purposes of treatment, payment, or health care operations. PHI is defined as health information related to the “past, present, or future physical or mental health” of an individual, which identifies that individual (by any one of eighteen identifiers), and is transmitted or maintained in any form or medium.

The Rule recognizes that covered entities cannot perform all required services in-house, so it permits the disclosure of PHI to contractors and vendors, called Business Associates, who provide services in which access to PHI is required. Contractors such as those engaged in transcription of medical information and technical support for electronic medical record and billing systems would be considered Business Associates, as they perform services on behalf of the covered entity, and require access to PHI to fulfill their tasks. In order to provide the required PHI to the Business Associate, the covered entity and the Business Associate must enter into a contract called a Business Associate Agreement, in which...
the Business Associate agrees to keep
the PHI confidential, according to certain
enumerated provisions of the Rule.20

In most instances, providers and plans
will not directly contract with offshore
vendors but, instead, will enter into
Business Associate Agreements with
domestic concerns which, in turn, may
sub-contract to offshore outsourcing
providers. The Rule permits such sub-
contracting, provided the subcontractor
provides assurances that it will follow
the same confidentiality requirements
(i.e., provisions of the Rule) to which
the Business Associate has agreed to
be bound.21 It is not a stretch to surmise
that many Business Associates will fail
to obtain such assurances. If they
obtain them from vendors in countries
which do not have adequate privacy
protections, these assurances may be
hollow at best.

Accountability for the acts of a subcon-
tractor is somewhat attenuated.22 The
Office of Civil Rights of HHS (“OCR”),
which enforces the Rule, has no juris-
diction over Business Associates. There
is no obligation on the part of a cov-
ered entity to monitor the conduct of its
Business Associate, let alone a subcon-
tractor in the U.S. or abroad.23 A cov-
ered entity must, if it finds out about a
“material breach or violation of the con-
tract by the business associate, take
reasonable steps to cure the breach or
end the violation, and, if unsuccessful,
terminate the contract with the business
associate.” If termination is not feasible,
the covered entity must report the prob-
lem to OCR.24

Dissemination of PHI over the Internet,
such as the transmission of a patient’s
file by UCSF Medical Center’s Pakistani
sub-contractor over an unsecured and
unencrypted e-mail, would certainly be
a material breach and violation of the
contract. If a covered entity failed to
take the steps above, and a patient
filed a complaint with OCR, the covered
entity could be liable for significant civil
monetary penalties under the Rule. The
covered entity would have little recourse
against a subcontractor beyond the
reach of U.S. law, though it may protect
itself by inserting indemnification and
hold harmless provisions in its contract
with the Business Associate. These may
provide only cold comfort, however, if the
Business Associate is judgment proof
due to bankruptcy or other reasons.

It may be advisable, in this current cli-
mate, for covered entities to keep PHI
within American borders or countries
with strong privacy protections, such as
those of the European Union,25 and
insert into their Business Associate
Agreements provisions that PHI may
not be subcontracted to vendors in
countries which lack strong privacy
protections (and to list those countries).

State Laws
Little comfort should be derived from
the lack of a private right of action
under HIPAA, as such a right exists
under certain state confidentiality laws.26
Further, state laws which are more strin-
gent in the protection of medical priva-
cy than HIPAA are not preempted by
the Privacy Rule.27 A bill is pending in
California requiring consumer consent
prior to the transfer of medical data to
offshore outsourcing providers.28

Several states at present have statutory
or common-law provisions for a right of
action for violation of medical confiden-
tiality, based upon fiduciary obligations.29
In McDonald v. Clinger, a New York
state intermediate appellate court deci-
sion citing Washington and Ohio law,
the court stated:

It is obvious then that [the physician-
patient] relationship gives rise to an
implied covenant which, when
breached, is actionable . . . The rela-
tionship of the parties here was one
of trust and confidence . . . Defendant’s
breach was not merely a broken con-
tractual promise but a violation of a
fiduciary responsibility to plaintiff
implicit in and essential to the doctor-
patient relation.30

This decision has been cited as a basis
of a right to sue by courts in Florida
and Pennsylvania.

Liability of health care providers and
plans under state law for improper dis-
semination of identifiable health data by
foreign affiliates can be argued under
traditional agency principles, and could
also be upheld on policy grounds
involving breach of confidentiality.

For example, New York’s statute pro-
tecting HIV/AIDS information contains
more stringent protections than HIPAA,31
and a state intermediate appellate
court in the case of Doe v. Roe,32 has
held that there is private right of action,
including claims for punitive damages,
where there has been disclosure of
HIV/AIDS information in violation of
these provisions. The court referred to
the strong public policy for confidential-
ity as a means to encourage affected
individuals to come forward and seek
treatment, as articulated in the statute,
and also noted that “. . . the Governor’s
Bill Jacket regarding enactment of
Section 27-F [of the Public Health Law]
indicates that the Legislature intended
to create a private cause of action to
remedy violations of that article.”33

Thus, it is eminently foreseeable that
health care providers and health plans
who outsource identifiable medical
information to offshore providers who
improperly release it could well be
found liable in state court actions for
substantial monetary damages.34 With
their offshore providers beyond the
reach of U.S. indemnification proceed-
ings, providers and plans could be left
holding a rather large bag.
Offshore Outsourcing

Federal Proposals

In concerns about privacy lapses by offshore providers, the media have found an issue for this election year that dovetails neatly with the angst over the loss of white-collar jobs. A reporter for The Boston Herald wrote last November that "[t]he hot-button issue [outsourcing] has risen to the level of presidential politics, with U.S. Senator John Kerry (D-Mass.) proposing a "Call Center Consumer’s Right To Know Act," designed to protect the jobs and privacy of Americans." With so much attention under the klieg lights of an election year, Congressional action was sure to follow. Indeed, Congressman Edward Markey (D-Mass.) was quoted in the article as stating "[t]hey started off sending American jobs overseas. Now Americans get to lose their jobs and their privacy at the same time." This heightened public attention may change the liability landscape for businesses which send medical data to offshore providers. Congressman Markey has introduced a bill which would require the consent of health care consumers before their medical data can be offshored to countries without adequate privacy protection, and would provide for a state private right of action "if otherwise permitted by the laws or rules of court of a State" for actions in violation of this Act. This bill also confers a right of action on behalf of a state in federal court. The Federal Trade Commission must be given notice of a proposed action by a state, and shall have the right to intervene. There is an explicit provision for punitive damages in the state court right of action.

Senator Clinton’s bill, known as the "SAFE-ID Act," defines “health care business” as “any business enterprise or private, nonprofit organization that collects or retains personally identifiable information about consumers in relation to medical care...” and includes hospitals, health maintenance organizations, medical transcription companies, banks that collect or process medical billing information, and subcontractors or potential subcontractors of those entities. Consent is required in order for a health care business to transmit personally identifiable information to a country without adequate privacy protection. That term envisions certification of countries with such protection, defined as countries that have “legal systems that provide adequate privacy protection for personally identifiable information.” The bill contains an explicit private right of action against a health care business for the actions of its “foreign affiliates or subcontractors,” for damages “arising from the improper storage, duplication, sharing, or other misuse of personally identifiable information...”

The pace of transition from paper to electronic medical records (“EMR”) has been prodded by the Executive and Legislative branches of government. It will serve to highlight privacy concerns, as health care entities and their IT affiliates look offshore in their quest to balance the increase in back-office tasks such as database administration, technical support, and billing with the managerial imperative to control costs.

The EMR movement enjoys bipartisan support. President Bush argued in a Radio Address on January 24, 2004:

My budget for the coming year proposes doubling to $100 million the money we spend on projects that use promising health information technology. This would encourage the replacement of handwritten charts and scattered medical files with a unified system of computerized records. By taking this action, we would improve care, and help prevent dangerous medical errors, saving both lives and money. A Presidential Advisory Committee has proposed a series of draft recommendations with regard to the transition to EMR. As these recommendations are perhaps not unrelated to the fact that in 2000 President Bill Clinton’s Quality Interagency Task Force proposed computerization of medical records as a means to reduce medical errors.

Senator Edward Kennedy has proposed legislation which would provide incentives for the transition, but would also institute penalties for those who do not make the transition to EMR. The bill envisions a “clinical informatics system” which would, among other things, incorporate “error notification software so that a warning is generated by such system if an order is entered that is likely to lead to a significant adverse outcome for the patient” and “allow the secure electronic transmission of information to other health care providers.” Not surprisingly, the legislation would direct the Secretary of Health and Human Services to adopt standards relating to “the protection of confidentiality” consistent with the HIPAA Privacy Rule.

The private sector can always be relied upon to detect new opportunities in health care technology, but it has been the experience of healthcare lawyers that opportunities often create headaches. One startup company has developed a Radio Frequency Identification (“the RFID”) patient bracelet, which will provide the patient’s information by radio signals from a silicon chip and tiny antenna via wireless transmission (“Wi-Fi”) from a local area network (“LAN”) to a physician or nurse with a Tablet PC or PDA. The company predicts the product can significantly decrease the incidence of medical errors. Following closely on the heels of products such as these, an Indian “global outsource company” is actively seeking RFID clients for data tracking...
and collation functions at its 6,000 employee Bangalore campus.49

In a recent study on offshore outsourcing for the financial services industry, the Federal Deposit Insurance Corporation (“FDIC”) listed India among countries with “no general data protection law.”50

Potential Solutions as Double-Edged Swords
The pace of offshore outsourcing is not likely to diminish. How, then, may health care providers and plans protect themselves from liabilities associated with the risk of disclosures by providers beyond the reach of U.S. law?

Prohibit all offshore outsourcing of medical data
This may be an expedient solution but, given the potential enormity of cost savings, the idea has rather short political legs. The proposal by California State Senator Liz Figueroa to do just that,51 was amended down to a disclosure and consent requirement for offshore outsourcing,52 then to one which permits a civil action against the originator of protected information for violation of the state privacy law “regardless of where the violation occurs.”53

A total ban on offshore outsourcing of medical data, this political odyssey indicates, is unlikely, particularly in an era in which health care entities are starved for in-house resources and are scraping to save every dollar possible.54 In addition to being vulnerable to cries of protectionism, such legislation prohibiting offshore outsourcing of medical data could, arguably, result in an increase in health care costs — not a palatable prospect in an election year.

Contracts with strong indemnification and hold-harmless provisions
Good fences may make good neighbors, as Robert Frost wrote, but one must have the threat of recourse to keep the neighbor from crossing the fence. Indemnification and hold-harmless clauses are not even enforceable uniformly across the U.S. In countries with weak or nonexistent court systems, they may well be quixotic at best. A potential remedy for this problem may be a requirement for a bond, or an insurance policy naming the provider as an insured. Of course, the raison d’être for offshore outsourcing is its low cost, which is occasioned by the location of providers in countries with low labor costs.55 These factors should indicate that outsourcing providers in those countries probably could not afford either a bond or the cost of insurance.

Contracts which require that the domestic Business Associate bear the liability for the actions of its offshore providers
This concept envisions enforcement of indemnification agreements in U.S. courts, and puts the onus on the Business Associate to monitor the activities of the offshore provider. Health care entities, though, may then face the prospect of increased costs if their Business Associates pass back the expenses in monitoring subcontractors and procuring additional insurance to protect the Business Associate against suits or claims for the actions of the offshore providers. The Business Associates face a Hobson’s Choice, both resulting in the need to raise their prices: they can meet the contractual standards by purchasing additional insurance to defend against misconduct of their foreign subcontractors, and increase their vigilance on the activities of the offshore providers; or they can keep all the subcontracted work in the U.S. which, of course, is more expensive.

Legislation permitting a private right of action against health care providers and plans in the event of improper disclosure by their foreign affiliates
The political climate appears favorable for such action, in the wake of the UCSF incident, but the current administration is litigation-averse and thus the proposals by Senator Clinton and Congressman Markey may not get much traction. Indeed, a cogent argument can be advanced that, given the network of state and federal privacy laws which could be brought to bear upon an improper dissemination of health data overseas, as analyzed above, there is no need to create a new federal cause of action. Proponents of such legislation may argue, though, that the very diversity of state remedies highlights the need for consistency in the approach to privacy; indeed, this was the one of the rationales behind the HIPAA Privacy Rule.

The Financial Services Model
The health care industry, it can be argued, learned outsourcing at the knee of financial institutions, and it is the financial industry which has taken it upon itself, largely by virtue of the existing network of laws governing the security of financial data, to seek a more coherent solution.

The financial services industry has many years of experience in traditional outsourcing to domestic third-party service providers, but the practice has grown significantly in the past few years due to the increased reliance upon Information Technology (IT), combined with competitive pressure to lower costs for those services.56 A web of federal statutes protects the security of financial data by requiring financial institutions to take steps to safeguard that information. Accordingly, legislators have taken a proactive approach to the
Offshore Outsourcing  Continued

privacy of electronic data. In a letter to Congressman Edward Markey, responding to his questions about how such information can be safeguarded when it has been outsourced to third-party service providers beyond the reach of U.S. law, Federal Trade Commission (“FTC”) Chairman Timothy Muris wrote “[s]imply because a company chooses to outsource some of its data processing to a domestic or offshore provider does not allow that company to escape liability for any failure to safeguard the information adequately.”63

The FTC has jurisdiction to enforce such provisions as the Gramm-Leach-Bliley Act,58 (security of financial information, and some health data corollary to financial information), the Fair Credit Reporting Act,59 the Children’s Online Privacy Act,60 and the Telemarketing Sales Rule (the National Do Not Call Registry).61 The Chairman’s comments appear to indicate that the FTC intends to take an active approach to improper disclosure of private financial data. Indeed, in his May 7, 2004, letter the Chairman noted that “the duty to protect customer information” in the Gramm-Leach-Bliley Privacy Rule “also applies to information handled or maintained by the financial institution’s affiliates.”62

While highlighting the FTC’s awareness of the privacy risks posed by the offshore outsourcing of sensitive data, the Chairman was constrained to point out that none of the aforementioned statutes provides for a private cause of action and stated — his statement notwithstanding — “Thus far, the agency has not brought a law enforcement action based on the failure of a service provider — here or overseas — to protect information.”63

In June, 2004, the Federal Deposit Insurance Corporation (“FDIC”) commissioned a study on consumer privacy risks associated with offshore outsourcing by insured financial institutions (“the Report”).64 One of the bases for the study was that consumers do not, under the Gramm-Leach-Bliley Act, have the opportunity to opt out of a transfer of their information overseas when the purpose of the transfer is to “service or process a financial product that the customer requested or authorized; or maintain or service the customer’s account.”65 These functions make up a large number of transactions, and the consumers’ inability to refuse transfers to countries with little or no privacy protection, coupled with the Report’s estimate that “$356 billion, or 15 percent, of the financial service industry’s current cost base is expected to move offshore within the next five years,”66 gave added impetus to the study.

The FDIC looked at several countries in which offshore data service providers are based. It noted that while countries of the European Union had privacy protections equivalent to those in the U.S.,67 such widely-used offshore provider locations as India, China, Philippines, Singapore, Malaysia, and South Africa have no general data protection.68

As the health care industry moves toward complete transition to electronic health records in the next ten years,69 it will face many of the same privacy concerns and risks which have confronted financial institutions. Thus, the recommendations of the FDIC with regard to consumer privacy risks can serve as a model for health care entities in the coming years. These recommendations, propounded for “institutions that are considering offshoring decisions,” include:

- Assessments of privacy risks for the offshore provider country;
- Ongoing oversight of all third-party providers, their activities and the status of data protection in the provider country, including the use of independent audit reports;
- Contract provisions which protect the privacy of consumers and their data, including, choice of law; prohibition on use or disclosure of offshore data except to carry out the contracted services; and local legal review of the contract to determine enforceability of all aspects of the contract;
- Establishment of a Central Database “to assist in monitoring the systemic risk posed by foreign technology service providers.” Legislation would require entities to notify the agency in charge of the database within thirty days of the existence of the foreign service relationship. The database would assist those charged with enforcing the privacy provisions (Office of Civil Rights, in the case of health care) with monitoring and investigating privacy issues.69

Conclusion

The last of these recommendations requires federal legislation, but counsel for health care entities can, by assiduous drafting of Business Associate Agreements and subcontracts, presently reduce the exposure which will accompany the increasing use of foreign health data service providers. We will be hearing a lot about outsourcing in the coming months of the presidential campaign. Media highlighting of privacy issues such as those described above raises public awareness of privacy issues, and could well result in an expansion of claims for improper disclosure. With proactive steps to mitigate those risks, erosion of the cost savings from the seemingly inevitable transfer of private health information offshore by fines and damages awards from improper disclosure of that information overseas can be mitigated.
This article appeared in the ABA Health Law Section’s The Health Lawyer (vol. 16, no. 6, August 2004, p. 24-30). Article Copyright © 2004 American Bar Association. This information or any portion thereof may not be copied or disseminated in any form or by any means or downloaded or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

This communication is published as an information service for clients and friends of the firm and is made available with the understanding that it does not constitute the rendering of legal advice or other professional service. © 2004 Sedgwick, Detert, Moran & Arnold LLP

2 Federal Deposit Insurance Corporation, Offshore Outsourcing of Data Services by Insured Institutions and Associated Privacy Risks (June 2004).
3 Id. at 2.
7 Davis, supra note 1.
8 David Lazarus, Outsourced UCSF Notes

10 Id.
11 Lazarus, supra note 8, at A23.
12 Lazarus, supra note 9, at A1.
13 Id.
16 45 C.F.R. § 160.103(3).
17 45 C.F.R. § 164.502(a).
19 45 C.F.R. §§ 160.103, 164.504(e).
20 45 C.F.R. § 164.504(e).
21 45 C.F.R. § 164.504(e)(2)(ii)(D).
22 In a letter from Tommy G. Thompson, Chairman, Department of Health and Human Services, to Congressman Edward J. Markey, Chairman Thompson noted that the Office of Civil Rights had only one case which alleged improper disclosure of protected health information overseas. The case cited a report involving the subcontractor of an overseas business associate which provided medical transcription services for a covered entity. Letter from Tommy G. Thompson, Chairman, Department of Health and Human Services, to Edward J. Markey, Congressman 2 (June 14, 2004), available at http://www.house.gov/markey/healthprivacy.htm.
24 Id.
27 45 C.F.R. § 160.203(b).
29 MONT. CODE ANN., §§ 50-16-525, 50-16-553 (authorizing a private right of action against a provider and its agents); WYO. STAT. ANN. §§ 35-2-606, 35-2-616 (authorizing a private right of action against a hospital and its agents).
31 N.Y. PUB. HEALTH LAW § 2780, et seq. (McKinney 2004).
33 599 N.Y.S.2d at 352-53.
34 See CAL. CIV. CODE § 56.36 (allowing a private right of action against “any person or entity who has negligently released confidential information.”); MD. CODE ANN., HEALTH-GEN. § 4-309(f) (“A health care provider or any other person who knowingly violates any provision of [the Confidentiality of Medical Records] statute is liable for actual damages.”); MONT. CODE ANN. §§ 50-16-525, 50-16-553 (authorizing a private right of action against a provider and its agents); WYO. STAT. ANN. §§ 35-2-606, 35-2-616 (authorizing a private right of action against a hospital and its agents); TEX. HEALTH & SAFETY CODE ANN. § 241.156. The relevant section of the statute states, “[a] patient aggrieved by a violation of this subchapter relating to the unauthorized release of confidential health care information may bring an action for: (1) appropriate injunctive relief; and (2) damages resulting from the release.” Thus, the statute appears not to place limits on a patient’s
Offshore Outsourcing  Continued

right to sue. Id; see also Warner v. Lerner, 348 Md. 733, 705 A.2d 1169 (Ct. of App. 1998) (holding that the plaintiff stated a claim under Maryland’s Confidentiality of Medical Records Act where plaintiff alleged that doctor who had not treated the plaintiff disclosed the plaintiff’s medical records).

35  Fitzgerald, supra note 14, at Finance 27.

36  Id.


38  S. 2312 § 2.

39  Id. § 5.

40  Id. § 3.

41  Inappropriate disclosure of Protected Health Information by a foreign outsourcing provider or other subcontractor, though, would probably not violate applicable provisions of the Electronic Communications Privacy Act. 18 U.S.C. § 2702 (2004). Section 2702 states “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” While a court may hold that a subcontractor which provides IT services to a covered entity provides an “electronic communication service,” the court would also likely find that the subcontractor did not provide this service to the public. See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998) (holding that Andersen Consulting, which maintained an interoffice e-mail system for UOP’s internal communications, could not be liable under § 2702 because its electronic communication service was not open to the public).

42  PITAC, supra note 4, at 6.

43  Id. at 2.


45  S. 2421.

46  Id. § 101(a)(2).

47  Id. § 101(d)(3).


50  Federal Deposit Insurance Corporation, supra note 2, at 20.

51  California Likely to Ban Medical Data Outsourcing, DECCAN HERALD, November 23, 2003.

52  Lazarus, supra note 8, at A23.


54  The Federal Deposit Insurance Company, in a recent study, noted that “[c]ompetitive pressures are the primary motivator for financial institutions to move higher-risk functions offshore.” Federal Deposit Insurance Corporation, supra note 2, at 2.


56  Federal Deposit Insurance Corporation, supra note 2, at 2.


62  Muris, supra note 57, at 5 n.15.

63  Id. at 6.

64  Federal Deposit Insurance Corporation, supra note 2.

65  Id. at 13, (citing § 502(e) of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(e) (2004)).

66  Id. at 2.


68  Id. at 20-22.


70  Federal Deposit Insurance Corporation, supra note 2, at 15-20.

Kenneth N. Rashbaum is a partner in the New York office of Sedgwick, Detert, Moran & Arnold LLP. He is the Chairman of the firm’s HIPAA Task Force and concentrates his practice in healthcare compliance and litigation.

The author gratefully acknowledges the research and editorial assistance of Todd Spiegelman in preparation of this article.

Kenneth N. Rashbaum can be reached at:

212.422.0202
125 Broad Street, 39th Floor, New York, NY 10004-2400
kenneth.rashbaum@sdma.com