PRACTICE RESOURCE

Offshoring Health Information: Issues and Lingering Concerns

Allen Briskin, Lisa C. Earl, Gerry Hinkley, and Joseph E. Kendall

Allen Briskin is Senior Counsel at Pillsbury Winthrop Shaw Pittman LLP. He advises for-profit, nonprofit, and government health care clients in organizational, regulatory, corporate, and business matters, emphasizing health information privacy and security, hospital operations and hospital-physician alignment, and managed health care. Contact him via email at allen.briskin@pillsburylaw.com.

Lisa C. Earl is Counsel at Pillsbury Winthrop Shaw Pittman LLP. She advises in multinational sourcing transactions, commercial arrangements, and complex service and procurement transactions, including software licensing and commercialization; technology asset sale and acquisition; IT systems and software; data center services; and fiber procurement and maintenance. Contact her via email at lisa.earl@pillsburylaw.com.

Gerry Hinkley is a Partner at Pillsbury Winthrop Shaw Pittman LLP. He represents clients throughout the health care industry and regularly serves as general counsel for health care organizations, with responsibility for corporate law and board governance matters. Contact him via email at gerry.hinkley@pillsburylaw.com.

Joseph E. Kendall is a Partner at Pillsbury Winthrop Shaw Pittman LLP. He advises on complex technology transactions, including large-scale information technology sourcing arrangements, as well as business process and transformational outsourcing transactions involving domestic and offshore vendors. Contact him via email at joseph.kendall@pillsburylaw.com.

## Briskin, Earl, Hinkley, and Kendall: Offshoring

### CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>102</td>
</tr>
<tr>
<td>Is Offshoring Illegal?</td>
<td>103</td>
</tr>
<tr>
<td>HIPAA Risk Analysis</td>
<td>104</td>
</tr>
<tr>
<td>HIPAA Business Associates and Subcontractors</td>
<td>105</td>
</tr>
<tr>
<td>Medicare Advantage and Prescription Drug Plans</td>
<td>105</td>
</tr>
<tr>
<td>Recommended Implementation Guidelines</td>
<td>107</td>
</tr>
<tr>
<td>Addressing Offshoring Concerns in Vendor Contracts</td>
<td>109</td>
</tr>
<tr>
<td>Prior approval for offshoring</td>
<td>109</td>
</tr>
<tr>
<td>Compliance with security policies</td>
<td>110</td>
</tr>
<tr>
<td>Security at the offshore location</td>
<td>111</td>
</tr>
<tr>
<td>Incident reports</td>
<td>112</td>
</tr>
<tr>
<td>Personnel issues</td>
<td>112</td>
</tr>
<tr>
<td>Approval for relocation of offshored services</td>
<td>113</td>
</tr>
<tr>
<td>Disaster recovery and business continuity</td>
<td>115</td>
</tr>
<tr>
<td>Cybersecurity insurance</td>
<td>116</td>
</tr>
<tr>
<td>Other considerations</td>
<td>116</td>
</tr>
<tr>
<td>Conclusion</td>
<td>116</td>
</tr>
</tbody>
</table>
Introduction

Health care providers, payers, and the organizations that provide business services to them may encounter offshoring arrangements in a variety of situations. In offshore arrangements, a health care organization’s electronic information, which may include confidential business information as well as protected health information (PHI) or other personal information, is either maintained outside the United States or made accessible to persons located outside the United States. Offshoring issues commonly arise in arrangements with vendors that provide billing, customer service, transcription, or information management from locations outside the United States. Offshoring issues also can arise when a vendor, or the vendor’s subcontractor, stores information offshore or makes information stored in the United States accessible to individuals who are located offshore.

Sometimes the offshoring arrangement is readily apparent, such as when a vendor agrees to provide services from a specified center located outside the United States. In other situations, the presence of offshoring issues may be less immediately apparent. For example, a vendor may provide its direct services to a health care organization from a location inside the United States, but may have maintenance or after-hours support provided from offshore locations, giving individuals located offshore access to a health care organization’s information.

Health care organizations’ counsel should take steps to address legal and policy requirements that may attach and employ offshoring-specific diligence and contractual protections. They should familiarize themselves with likely situations in which offshoring can occur and inquire of vendors specifically whether offshoring may take place. Failing to identify and address offshoring arrangements can expose the organization to increased risks of data breaches and other privacy violations, or cause it to breach contractual obligations to third parties.
that have required that the organization take special measures regarding offshoring.

This Practice Resource discusses the legality of offshoring and contexts in which offshoring arrangements should be addressed specifically, i.e., in connection with risk assessments under the Health Insurance Portability and Accountability Act (HIPAA), business associate contracting, and arrangements with Medicare Advantage and Prescription Drug plans. This Practice Resource then provides implementation guidelines for addressing offshoring situations, as well as specific provisions that can be adapted for use in contracts that involve offshoring.

**Is Offshoring Illegal?**

Offshoring is not illegal, but it raises a number of business, compliance, and other legal issues that have led some to believe that health care organizations should not offshore information and should prohibit their vendors or other contracting parties from doing so. Offshoring arrangements raise concerns because of misconceptions surrounding whether the arrangements are permitted. Locating facilities or personnel outside the United States makes it more difficult and expensive to conduct pre-contracting due diligence or ongoing monitoring of performance. Time zone differentials may limit the immediacy, if not the overall effectiveness, of communications between the health care organization and offshore personnel or facilities. Finally, if the arrangement involves contracting with a vendor located outside the United States, concerns may arise about its legal and practical enforceability, including whether the health care organization will be able to successfully assert jurisdiction over a party in a foreign country, or whether government agencies will be able to enforce U. S. laws and regulations across national borders.
HIPAA Risk Analysis

While HIPAA does not prohibit offshoring, offshoring concerns should be taken into account in performing the risk analysis required under HIPAA’s Security Rule. Following the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act and the 2013 HIPAA Omnibus Final Rule (Omnibus Rule), each HIPAA-covered entity and business associate must conduct, and periodically update, a “risk analysis” that accurately and thoroughly assesses the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by that covered entity or business associate. When that covered entity or business associate stores PHI offshore or allows its vendors or other subcontractors to access that information from offshore, the potentially unique risk that can arise from such an arrangement should be taken into account in the risk analysis. The risk analysis also should address the physical and technical safeguards the vendor can employ to comply with its HIPAA business associate obligations, as well as the vendor’s ability to assimilate its local customs and standards into a HIPAA compliant environment, especially one that can be assessed from afar. Practically speaking, a health care organization should examine its offshore business associates closely to grasp:

- the potential impact of local legal standards for health information privacy,
- the technical environment in which the information will reside,
- the ability to assess in real time whether privacy and security standards are continuously adhered to, and
- its own ability to enforce contractual safeguards under the laws of a foreign jurisdiction.

1 45 C.F.R. § 164.308(a)(1)(ii).
3 45 C.F.R. § 164.308(a)(1)(ii).
HIPAA Business Associates and Subcontractors

Covered entities and business associates must base their privacy and security infrastructures on the HIPAA Privacy and Security Rules, but should not consider compliance the last word on privacy and security. The Omnibus Rule expanded the definition of “business associate” to include individuals and entities that, other than as a member of a party’s workforce, creates, receives, maintains, or transmits PHI in the performance of a function or activity for a covered entity or another business associate. The Omnibus Rule incorporated changes made by the HITECH Act to require that business associates comply with HIPAA’s Security Rule and certain provisions of HIPAA’s Privacy Rule and Breach Notification Rule. As a result, business associates must consider the obligations they wish to impose on subcontractors regarding the privacy and security of electronic information. Following the Omnibus Rule, business associates must consider not only how they will perform the business associate obligations they owe to covered entities, but also the business associate obligations they should impose on their vendors and other subcontractors. As business associates contemplate their own business associate contracts with subcontractors, they should consider whether the arrangements address issues, such as those raised by offshoring, that are not fully addressed by HIPAA.

Medicare Advantage and Prescription Drug Plans

On July 23, 2007, the Centers for Medicare and Medicaid Services (CMS) issued a memorandum (CMS Memorandum) to current and prospective Medicare Advantage plans and Prescription Drug plans (collectively, sponsors) that requires sponsors to survey arrangements by their vendors and other contractors that “receive, process, transfer, handle, store, or access beneficiary [PHI] in oral, written, or

4 45 C.F.R. Part 164, Subparts E and C, respectively.
5 45 C.F.R. §§ 164.302, 164.500(c).
 electronic form,” and to report on those activities to CMS.⁶ In that memorandum, CMS stated: “Given the unique risks associated with the use of contractors operating outside the jurisdiction of the United States, CMS encourages sponsors using offshore subcontractors to take extraordinary measures to ensure that offshore arrangements protect beneficiary privacy.”⁷

CMS has not, however, published regulations that describe what those “extraordinary measures” are supposed to be. Instead, the CMS Memorandum included an “Offshore Subcontract Information and Attestation” form that each sponsor is to complete for each vendor that either is located outside the United States or makes PHI available for access outside the United States. The attestation form solicits a variety of information about specific measures the sponsor may have taken to address the risks of offshoring, including a description of the alternatives to offshore contractors the sponsor considered and why each alternative was rejected. Although CMS collects these attestations from participating organizations, it has stated it does not evaluate or issue written approvals of sponsors’ subcontracting arrangements.⁸ CMS has not prohibited offshoring arrangements.

The attestation form requires the sponsor to state whether certain measures are in place to safeguard PHI. Neither the CMS Memorandum nor the attestation form states that any of these measures are required, but the implication appears to be that CMS believes these measures represent the minimum safeguards. Health care organizations should treat the CMS attestation as guidance for the minimum

---

⁷ Id.
⁸ Memorandum from Cynthia Tudor, Dir., Medicare Drug Benefit Group, CMS, to All Part D Plan Sponsors, Sponsor Activities Performed Outside of the United States (Offshore Subcontracting) Questions and Answers (Sept. 20, 2007).
elements of a plan for structuring and managing offshoring arrangements. The following recommended implementation guidelines for offshoring arrangements are based in large part on the CMS attestation form and would address all the issues that CMS has raised therein.

**Recommended Implementation Guidelines**

Based on the issues raised by offshoring and the guidance provided by the CMS attestation process, the following guidelines for offshoring arrangements have emerged.

1. Health care organizations and their vendors should adopt measures to collect, document, and maintain relevant information to identify offshore arrangements, impose appropriate measures in a consistent and orderly way, monitor compliance, and take action if problems arise. For example, they should consider prohibiting vendors from using offshoring arrangements without the health care organization’s prior written approval and require vendors to provide specified reports regarding offshoring arrangements generally and privacy and/or security problems specifically.

2. Covered entities and business associates should enter into HIPAA-compliant business associate contracts, including the demand that business associates’ do the same with their subcontractors that create, receive, maintain, or transmit protected health information. At the same time, covered entities and business associates should develop and implement other appropriate measures to address privacy and security issues not addressed by HIPAA, such as offshoring issues, incorporating those measures into their contracts, and requiring that business associates do so in their subcontracts.

3. Contracting arrangements with vendors and others that engage in offshore activities should include measures to
ensure that electronic information, including confidential business information and PHI—as well as individuals’ other personal information—remains secure and is protected from unauthorized access, use, disclosure, modification, destruction, or otherwise being made unavailable. For example, contracts should require vendors or other contractors to comply with specified privacy and/or security policies and procedures adopted or approved by the health care organization or vendor, such as those suggested below.

4. Offshore contracting arrangements should prohibit the offshore contractor’s access to data that it does not require to perform its services for the health care organization, essentially extending HIPAA’s minimum necessary rule to a broader range of the organization’s information.

5. Offshoring contracts should include policies and procedures to address the organization’s response to data breaches or other matters of non-compliance. HIPAA requires that a business associate contract be subject to termination if the business associate violates a material contractual term. Health care organizations should consider whether expanded termination rights are appropriate when offshoring is involved, such as permitting termination following a data breach, even absent proof that a violation of the business associate contract caused the breach.

6. Contracts with vendors in offshoring arrangements should include all language required by applicable laws and regulations, including the HIPAA Privacy and Security Rules and, if applicable, the Medicare Advantage and Prescription Drug program regulations and contracting manuals. These requirements include: (i) acknowledging the powers of CMS and the Department of Health and Human Services, the Comptroller General, and others to inspect the
organizational’s books and records; (ii) complying generally with applicable Medicare rules; (iii) holding Medicare beneficiaries harmless from the sponsor’s financial obligations; (iv) allowing the sponsor to monitor the vendor’s performance on certain core functions delegated to the vendor; and (v) allowing the sponsor to revoke that delegation if the vendor does not perform satisfactorily.

7. The health care organization should annually or regularly audit offshore subcontractors and use those audit results to evaluate whether to continue its relationship with the vendor and whether corrective action plans or other measures are appropriate. Organizations should recognize that monitoring subcontractors’ activities may result in receipt of information that the subcontractors consider confidential or otherwise sensitive. The organization should take care to protect the confidentiality of that information.

8. Contracts with vendors should require those vendors to disclose all offshoring arrangements.

**Addressing Offshoring Concerns in Vendor Contracts**

Health care organizations can address many offshoring issues through contractual terms with the offshore service vendor. While a robust contract may not necessarily make the storage, processing, or accessing of offshore information more secure, it will give appropriate rights and remedies to the health care organization if offshoring leads to data protection issues.

**Prior approval for offshoring**

If the health care organization is contracting with a vendor located in the United States, offshoring still may occur if the vendor uses employees or contractors located in another country. In such cases,
the organization should have prior information about the potential offshoring so that it can reject any offshored services or—if the health care organization agrees to offshoring—impose conditions and requirements on the work performed offshore. This may have a cost implication on the services purchased, as use of offshore labor typically comes at a much lower cost than local labor.

Sample clause: Vendor will transfer, store, maintain, process or access all protected health information and other personal data only in and from the United States and will not transfer, store, maintain, process, or access Personally Identifiable Information in or from any other jurisdiction without Customer’s prior written consent.

Compliance with security policies

Even if the agreement specifies that the vendor must comply with the health care organization’s data privacy policies and applicable laws, it may be appropriate to reiterate that with respect to offshoring. Include the opportunity for the health care organization to change its privacy and security requirements from time to time based on actual or potential security issues arising due to the location where the offshored services are performed, or the type of data stored, processed, or accessed offshore. Topics typically covered in security policies include encryption, secure login and access management, removal and destruction of confidential information, anti-virus and malware protections, network access controls, security monitoring, and physical security.

Sample clause: Vendor personnel will not be permitted to access Customer data from, or transmit it to, offshore locations except in compliance with Customer’s privacy and security standards, policies and requirements, and applicable laws, including those relating to privacy, import-export controls and infor-
information, and data protection and security. Customer may establish, and Vendor will comply with, additional special privacy and security requirements and controls for offshore service delivery centers based on the specific Services that will be performed offshore and the types of Customer data that will be disclosed to Vendor personnel working there.

Security at the offshore location

Even if the health care organization’s data privacy policies incorporate security industry standards that the vendor must follow, it also may be appropriate to detail in the contract—with greater specificity than is used for a U.S. facility—the level of security that the health care organization expects at an offshore location. Other clients and vendors may use the same offshore facility, so segregation and specific protections of PHI and other personal data may be appropriate:

Sample clause: Vendor personnel will work in secured and physically partitioned areas within the offshore service delivery centers, separate from areas where work is performed for Vendor or Vendor’s other clients (a “Partitioned Work Area”). Partitioned Work Areas will be provided as part of the Services at no additional cost to Customer. Partitioned Work Areas will include the following features in addition to the work areas and space provided to Vendor personnel: (i) badge scan access and video surveillance; (ii) all laptops or desktops must be isolated logically to Customer’s network—they must not be connected to a public network or have the capability to copy or transfer data from Customer’s network to any other network, storage media, or device; (iii) a separate office for training, including video conference
capabilities so that Vendor personnel can interact with Customer personnel in a private manner; (iv) a secure area fax; (v) reasonable “overflow” space; and (vi) secure printing, photo-copying, and document shredding/disposal.

Incident reports

As the health care organization is less likely to learn about security issues encountered offshore through news, industry groups, and other sources, the vendor should provide visibility into the performance of its security controls at the offshore location. One way to achieve this is requiring the vendor to provide regular reporting on its security monitoring and any potential security breaches. The sample clause below requires the vendor to give the health care organization deeper insight into potential threats to which the offshore site is subject and the strength of security protections deployed by the vendor.

Sample clause: Each month during the Term, Vendor will provide Customer with a report regarding Vendor’s offshore service location detailing: (i) any network intrusions detected; (ii) any violations or attempted violations of physical security; (iii) details of any security violations (whether physical or logical) by Vendor personnel; and (iv) any other security-related incident that occurred during the month.

Personnel issues

Robust agreements require the vendor to undertake background checks of employees and subcontractors before an individual is permitted to provide services or have access to data. In some countries, the type and extent of background checks typically conducted in the United States may not be available or may be prohibited by law. For example, various privacy laws restrict the access and use of personal informa-
tion that would be uncovered through a background check, including Organisation for Economic Co-operation and Development Privacy Guidelines, the European Union Directive, the Asia-Pacific Economic Cooperation Privacy Framework, and the Canadian Personal Information Protection and Electronic Documents Act. Country-specific laws also impact the information that may be collected in background checks. For example, a prospective employer in Hong Kong is prohibited from obtaining a criminal history directly from crime enforcement authorities. These limitations and restrictions should not relieve the vendor from undertaking appropriate and lawful background checks:

**Sample clause:** Vendor’s reference checks and screening procedures for Vendor and contractor personnel assigned to perform Services offshore must satisfy customary reference checking and screening standards and procedures applicable to the country in which such individuals will be performing the Services.

**Approval for relocation of offshored services**

If the health care organization has approved offshoring as part of its arrangement with the vendor, the location from which the offshored services are provided must not change. If the vendor initiates change, then the health care organization will need to conduct further due diligence and protect itself from any costs arising from the change. Due diligence of any new location should include the same level of scrutiny that was given the initial offshore location, and should be conducted in accordance with a migration plan that the health care organization contributes to and approves. During migration, the parties should

9 From the Hong Kong Police Website: “The issuance of Certificates of No Criminal Conviction is a charged service provided by the Hong Kong Police Force which is solely in connection with a person’s application for a visa to visit or reside in another country, or for adoption of children. Applications for the Certificate for any other purposes will not be accepted.”
conduct testing of the new location to verify that service quality is not affected and security is not degraded. The vendor may wish to move the location of offshored services to gain cost efficiencies. In that case, it may be appropriate for the health care organization/customer to benefit from those cost efficiencies.

*Sample clause:* Vendor will perform the Services only at the Customer-approved service locations listed in [an attachment to the agreement]. Vendor may not change the location from which the Services are provided without Customer’s prior written approval, which Customer may grant or withhold in its sole discretion. Prior to seeking Customer’s approval of any proposed relocation, Vendor will prepare and submit to Customer a written evaluation of the effects of the contemplated relocation on the Services and on Customer. Vendor will have financial responsibility for all additional costs, taxes, and other expenses related to any Vendor-initiated relocation of a service location from which the Services are provided. Costs for which Vendor will be responsible may include Customer’s costs and expenses incurred during the conduct of due diligence, audits, and other inspections of the proposed new location. Vendor will manage any approved relocation in accordance with the Agreement and a written relocation plan prepared by Vendor and approved by Customer. The relocation plan will include provisions for comprehensive migration testing and require that Vendor perform all necessary tests to verify all of Vendor’s obligations under this Agreement continue to be met at all relevant times during and after the relocation. Vendor shall not relocate any work prior to successful testing of the location to which the Services are to be relocated.
Disaster recovery and business continuity

All supply contracts for critical services should address the vendor’s responsibility in the event of a catastrophic event affecting the site from which services are provided, including the creation, testing, and implementation of a robust disaster recovery plan, consistent with the principles of the International Organization for Standardization 22301. A disaster at an offshore site may necessitate transferring services to an alternative offshore location. In those circumstances, it may not be possible to carry out the type of due diligence performed for the primary offshore location’s back-up locations, but the health care organization at least should have a pre-approved list of alternate locations and the opportunity to assess them if appropriate. It would be impracticable for the vendor to go through the approval process suggested above before implementing the disaster recovery plan and moving production to another location. The contract therefore should provide some flexibility for business continuity, while providing as much protection as possible for the health care organization and its data:

Sample Clause: Vendor may temporarily relocate the Services to any of the locations listed in [an attachment to the agreement] to the extent necessary due to the occurrence of a force majeure event affecting the location from which Services are provided. During the temporary relocation to another offshore location, Vendor must continue to comply with all terms and conditions of this Agreement with respect to Services performed outside the United States. Vendor shall restore the operation of services from the original location as soon as technically possible. Any temporary relocation shall not exceed ten (10) days without the prior written consent of Customer.
Cybersecurity insurance

Most vendors will, at the request of a health care organization, agree to provide a level of cybersecurity insurance that should cover third party claims (including data security breaches, privacy breaches, and other liability) and first party losses (e.g., loss of data, revenue loss, and “e-extortion” costs). The insurance should cover the cost of credit monitoring, credit identity theft insurance, and other services corporate entities that maintain PHI make available to impacted individuals when a data breach occurs. Coverage for crises management expenses and regulatory response costs are equally important if services are performed offshore.

Other considerations

All other provisions in the services agreement, such as audit rights, a requirement to investigate and cooperate with the health care organization if there is a data breach, responsibility for costs of a data breach, etc., should apply equally to any offshore locations. Other considerations include operational and cost issues specific to offshore services, such as the high turnover rates of personnel in certain offshore jurisdictions. Some companies that use offshore vendors are concerned about corporate responsibility and accountability issues, such as working conditions, forced labor, and child labor. Those considerations are beyond the scope of this article, but deserve attention in the overall consideration of offshore services.

Conclusion

Third party supply contracts always require close scrutiny when the vendor will have access to PHI. The sample clauses above are intended to provide guidance on some of the additional terms and conditions that a health care organization should consider if any part of the vendor’s services will be performed, or data will be stored at or accessed
from, offshore locations. As offshoring services that require access to PHI becomes more common, counsel for health care organizations will be called upon to structure these proposed arrangements in a manner that safeguards, to the extent possible, both their organizations’ and patients’ best interests.