Outsourcing HIM Functions to Europe: A Perilous Atlantic Crossing

by Barry S. Herrin, JD, FACHE, and Jennifer D. Baxter

Somewhere in the United States, a small independent hospital contracts with an Irish company to code medical records for billing. The records are sent in electronic format to Ireland, where employees read and code the records and then return the coded records to the hospital. Bills are generated, submitted, and paid, saving thousands of dollars in coding costs. By all appearances, this is—or should be—a sound and relatively uncomplicated business transaction. Why isn't it?

The Scope of Directive 95/46/EC

In 1998 the European Union (EU) enacted Directive 95/46/EC, which governs the processing and movement of personal data. It directs its member states to enact legislation creating government data protection agencies and registration systems that provide a baseline level of security for personal data.

The directive operates from the premise that data processing is prohibited unless specifically allowed, a significant departure from American-style regulations, which traditionally provide that everything is permitted unless specifically prohibited. According to a strict reading of 95/46/EC, the hospital noted above is probably not entitled to have its data back from the coder without complying with 95/46/EC, and that may be difficult.

Directive 95/46/EC governs the electronic processing of personal data in the EU, regardless of where the data originated. The directive defines personal data as "any information relating to an identified or identifiable natural person," and the data subject as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[1]

There is no requirement that the data subject be an EU citizen. The burden of compliance is upon the data controller, defined as the "person or body which alone or jointly with another determines the purposes and means of the processing of personal information."[2] Processing is "any operation or set of operations which is performed upon personal data."[3] In our example, the Irish coding company would, if given discretion about how to "process" the data, become the data's controller.

The directive provides that personal data may only be processed for specific, authorized purposes and only as is adequate, relevant, and not excessive in relation to the purposes for which it was collected. This echoes HIPAA's "minimum necessary" restriction; however, 95/46/EC goes much further.

Every reasonable step must be taken to erase or rectify inaccurate or incomplete data. In addition, the data are not to be kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are processed. This is more restrictive than HIPAA, which permits a business associate to keep protected health information throughout the business relationship.

Also, unlike HIPAA, data subjects must be informed when their data are processed, including the controller's name and address, the purpose of processing, the recipients of the data, and all other information required to ensure fair processing. No such requirement exists under HIPAA for a hospital's outsourced coding relationships, and such need not be disclosed in a covered entity's notice of privacy practices.

Thus, in our example, the hospital would be required specifically to disclose the existence of the offshore coding arrangement to each patient whose data would be sent to Ireland.

Application of 95/46/EC to Third Countries

Directive 95/46/EC provides that the exchange of information with third countries may occur only if the third country ensures an "adequate level of protection in light of all circumstances," regardless of whether the third country is the source or owner of the data for purposes of intellectual property law.[4] However, some exceptions are enumerated.

The European Commission (EC) can deem that a country has an adequate level of protection and issue a standing order allowing for transfer of data. A transfer is permissible when the data subject consents unambiguously. (Acknowledging receipt of a facility's notice of privacy practices is not sufficient.)

A transfer is also permissible when necessary for the performance of a contract between the data subject and the controller (in our example, there is no direct contract between the patient and the coder) or when necessary for the performance of a contract concluded in the interest of the data subject between the controller and a third party (this might include the contract for healthcare services between the hospital and the patient).

A transfer is permissible when required on important public policy grounds (i.e., the law or public policy of the EU member state, not the third country, which has led to the inability of US companies to get data pursuant to court-ordered discovery). Finally, transfer is permissible to protect the vital interests of the data subject.

To ease the compliance burden on US companies wishing to exchange data with EU companies, in 2000 the US Department of Commerce and the EC agreed to a voluntary safe harbor program (SHP) for US organizations. The safe harbor provides a means for US organizations to become certified as adequately safeguarding data.

An organization may either join a compliant regulatory privacy program or develop a privacy policy that conforms to the safe harbor's requirements. An annual certification must be filed with the Department of Commerce.[5] Organizations are required to notify the department if their data protection system becomes noncompliant with the SHP, and persistent failure to comply may result in revocation of eligibility to participate.[6]

In theory, the SHP offers two critical advantages to US organizations. First, all EU states are bound by the EC's adequacy determination, meaning that individual state requirements are waived. Second, the SHP allows the Federal Trade Commission to enforce actions against US companies. The SHP is designed to be a simpler and less costly means of 95/46/EC compliance.

Limitations of the Safe Harbor Program

However, the SHP has its limitations. Only 45 domestic healthcare services organizations (DHSOs) are currently certified. No enforcement actions have been brought by the FTC to test the scope and protections of the safe harbor provisions.

There is also scant guidance from EU courts on the exchange of information with third countries, and existing cases favor a broad interpretation of 95/46/EC. Moreover, it is unclear whether a US company contracting with a DHSO will enjoy the protection that the DHSO enjoys, unless the company independently meets 95/46/EC standards.

The antiforwarding provision of 95/46/EC prohibits a DHSO from returning the data to its originator unless the originator is contractually bound to provide the same level of protection as the DHSO. This practically eliminates the benefit of using the DHSO. If a hospital can provide the same level of security as the DHSO, it can become certified and contract with the coder directly.

As a result, even if the hospital in our example were to contract with an IT "heavyweight" to facilitate this offshore coding contract, it most likely will still have limitations on retrieving its data.

Although the SHP grants US jurisdiction over enforcement proceedings, it does not solve the problem of potential civil suits between US organizations and the EU contractors. EU contractors will want the courts and laws of their member states (or the state with the most favorable law) to govern litigation. For this reason, US companies must be mindful of "choice of law" provisions when contracting.

If the parties cannot agree to US jurisdiction, the US company should consider an EU forum more favorable to US companies, such as the London Court of International Arbitration. More importantly, the US company must ensure that contracting dollars are well spent and that the contractor it selects provides the type, amount, and quality of services necessary.[7]

The implications for the hospital in our example and its thousands of dollars saved in coding costs remain unclear. However, the directive's language seems to indicate that a contractor's use of equipment in the EU to code medical record subjects these records to 95/46/EC. And, if our Irish coder exercises any judgment in processing the data, it becomes a controller bound to comply with 95/46/EC.

Directive 95/46/EC has no exception that allows the coder to return information to the hospital without compliance. Even if the hospital contracts with one of the 45 certified DHSOs, the antiforwarding provision means the hospital still cannot have access to its information after coding unless it is contractually bound to provide the same level of security as the DHSO. The hospital could argue that one of the exceptions to 95/46/EC applies (either under the specific consent exception or the exception for necessity for performance of a contract between the patient and the hospital), but that too remains unclear.

Reports indicate that the US and EU will announce a new agreement on data privacy, but for now the only clear thing is that relying on EU outsourcing contractors to manage or process data is risky and, for small and midsize companies, the risk may outweigh the reward.[8]

Notes

1. European Union. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data." 1995 O.J. (L281) 31.
2. Ibid.
3. Ibid.
4. Ibid, at Art. 25.
5. United States Department of Commerce. "Welcome to the Safe Harbor." Available online at www.export.gov/safeHarbor.
6. United States Department of Commerce. "Safe Harbor List." Available online at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.
7. Markus, Patricia A. "Picking the Right Health Information Solution." *Legal HIMformation,* July 2007. Available online at www.legalhimformation.com.
8. Savage, Charlie. "US and Europe Near Agreement on Private Data." *New York Times*, June 28, 2008. Available online at www.nytimes.com/2008/06/28/washington/28privacy.html?_r=1&oref=slogin.

Barry S. Herrin (barry.herrin@smithmoorelaw.com) is a partner in the law office of Smith Moore Leatherwood LLP, in Atlanta, GA. **Jennifer D. Baxter** is a third-year law student at the Georgia State University College of Law in Atlanta, GA.

Article citation:
Herrin, Barry S.. "Outsourcing HIM Functions to Europe: A Perilous Atlantic Crossing" *Journal of AHIMA* 79, no.9 (September 2008): 56-57; 62.