Chapter 5
Protecting Patient Information in Outsourced Telehealth Services:
Bolting on Security When it Cannot be Baked in

Patricia Y. Logan
Marshall University Graduate College, USA

Debra Noles
Marshall University Graduate College, USA

ABSTRACT

Hospitals have increasingly employed outsourcing to lower the cost of healthcare delivery and improve efficiency and quality, thereby, enabling more focus on core competencies of patient care, teaching, and research. Outsourcing presents a challenge for protecting patient information when new services are implemented or integrated into an existing healthcare information system. Enabling new outsourced telehealth services often requires "bolting on" security to legacy systems rather than "baking" it into the system. This chapter addresses security practices necessary for healthcare organizations implementing new telehealth services as part of an outsourced relationship. While a number of recommendations are available for security readiness assessments pursuant to HIPAA compliance, none directly addresses the challenge of implementing security for outsourced clinical services. A case study is presented for a recent implementation of teleradiology services within a large regional hospital. Using the case, system vulnerabilities are demonstrated and relevant best practices to mitigate exposing patient information are discussed.

INTRODUCTION

Multiple pressures exerted within the healthcare industry have driven the move toward outsourcing of clinical services. They include:

- rising costs of healthcare
- market competition
- need to focus on revenue generating core competencies (i.e., patient care, teaching, and research)
- lack of available specialists in key specialties (e.g., radiology)
- demand for quality healthcare services by the customers (Bedi, Sarma, & Arya, 2002)

The Hospital Outsourcing Trends in Clinical Services Survey (2006), questioned 266 executives from hospitals of all sizes, and reported 78% of the hospitals outsource at least one patient service, and 83% expect the level of outsourcing at their facilities to stay the same or increase over the next two to three years (Hill, Bartrum, & Guy, 2006). While hospitals have outsourced non-core activities, the clinical and diagnostics services have been slower to be adopted as outsource candidates (Outsourcing in Most Hospitals, 2007). Many clinical services have moved to offshore locations to realize greater cost savings and efficiencies (Goelman, 2007). In particular, a recent trend is to send patient radiological studies offshore to be interpreted by United States certified physicians. This process assists hospitals finding it increasingly difficult to attract and maintain on-site radiologists during evening hours. The need for such specialists has grown due to the increase in emergency room patients given scans to help diagnose their condition (Goelman, 2006; Levy & Goelman, 2005). Increasingly more common, the first interpretation of a radiology study is performed offshore in Europe or Australia with a second read done the following day within the hospital (Pollack, 2003).

The electronic delivery of sensitive data to offshore locations has sparked interesting security debates on how healthcare institutions should protect a patient's right to privacy. There are security implications and regulatory requirements at state, national, and international levels for hospitals entering into outsourced relationships. Equally important, hospitals must also determine if the security practices of the outsourced companies are acceptable. When the outsourced companies do not have adequate security for patient data, the hospital will be held liable, even if a breach of patient information happens at the third-party company. If hospitals do not protect the sensitive medical data traveling to third-party entities, the risk of exposing sensitive personal information to cybercriminals increases dramatically. The Identity Theft Resource Center (ITRC) reports that in 2007, almost four million patient records were exposed, representing 65 incidents and 14.9% of all breaches reported (Data Breach Report, 2007). While HIPAA represents the primary security guidelines for the United States, it does not mandate reporting of a security breach to patients. With no requirement for reporting, it is likely that the data from the ITRC significantly understates the actual occurrence of data loss from healthcare organizations.

The complexity of hospital data security management is a result of balancing the requirement to provide proper access to the data vs. the requirement to sufficiently protect the data. Clinical users expect the data to be available when it is needed, and view security as a secondary concern, especially in emergency scenarios. Presently, there is no guidance for hospitals involved in outsourcing clinical services in how best to comply with the security expectations of patients and regulatory agencies.

The goal of building any clinical information system is to improve the quality of patient care. The methods for protecting the data should not interfere. Hospitals must acknowledge patient data security is about risk management, and they