IRM PRESS
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com
ITB7479

Chapter 15

Information System Failures in Healthcare Organizations: Case Study of a Root Cause Analysis

Pamela E. Paustian, Donna J. Slovensky, and Jacqueline W. Kennedy
University of Alabama at Birmingham, USA

Preparedness for response and continued operation of a health care facility following an information systems disaster must encompass two facets: continuation of patient care delivery and continuation of business processes. This chapter reports a root cause analysis following an information system failure that compromised the organization's ability to capture clinical documentation for a 33-hour period.

INTRODUCTION

Delivery of health care is an information-intensive process, and the technology associated with data capture and information management is a critical operational and strategic resource. Most HCOs prepare formalized plans, policies, and procedures for recovery of computerized information system (IS) functionality and the recovery of any lost data following an IS disaster. Unfortunately, many disaster recovery plans are inadequate to guide action when a disaster occurs for a number of reasons. Conducting a root cause analysis in the aftermath of an IS disaster can be an important first step in evaluating the adequacy of existing recovery plans.

Previously Published in *Managing Information Technology in a Global Economy* edited by Mehdi Khosrow-Pour, Copyright © 2001, Idea Group Publishing.
This chapter appears in the book, Effective Healthcare Information Systems by Adi Armoni.

DEFINING DISASTER

In general usage, the term "disaster" describes an adverse event that occurs suddenly and unexpectedly. Terminology used to describe disasters within a specific context may incorporate several generic definitions to explain the contextual usage. Morris (1990) defined an automation-related disaster in a health care organization as "any situation that results in an automation support outage of sufficient duration to significantly disrupt hospital business and/or clinical services." This broad definition permits organization prerogative in designating the scope of information system disaster preparedness. This prerogative is not trivial as information systems in HCOs are both complex and dynamic. Information executives must make purposeful decisions about the time and financial resources expended to prepare and maintain disaster recovery plans – plans they hope never to implement. The degree of risk an organization accepts must be based on educated judgment about the likelihood given events will occur and the liability associated with failure to prepare for the eventuality.

INCENTIVES FOR IS DISASTER RECOVERY PLANNING

For hospitals, external disasters affecting the geographic market area served actually may increase the need to provide health care services. When the physical resources of the facility are compromised by environmental conditions, such as wind and water damage from a hurricane, delivery of care may become particularly challenging. Planning for and recovery from disasters, therefore, is mission-critical to HCOs. As HCOs are rapidly increasing their dependence on digital information capture and real-time data analysis to provide patient care, "protection of mission-critical information technology … is gaining serious attention" (Bandyopadhyay & Schkade, 2000).

The delivery of health services is information intensive and information dependent – from both clinical and business management perspectives. Loss of all or a portion of IS functionality quickly compromises clinical and business processes, and information is recognized as a key strategic resource in health care organizations (Kelly, 2000). Loss of stored data and information can have far-reaching effects, potentially including patient injury, legal liability, and significant financial loss to the organization. In short, the health care industry has become dependent on information technology to conduct its business – delivery of clinical care. Anticipating and preparing for management of and recovery from information system disasters is as mission-critical for health care organizations as is preparing for continuation of patient care in the event a disaster occurs. Determining the underlying cause of IS failure is a pivotal factor in assessing the adequacy of