Step 1. Outline

What	Problem(s)	Medical privacy breach
When	Date	September 9, 2010
	Time	?
	Different, unusual, unique	Use of contractor for billing
Where	State	California
	Facility, site	Hospital
	Task being performed	Providing data for homework site

Impact to the Goals

Patient Safety	N/A	
Employee Impact	N/A	
Compliance	Potential violation of HIPAA law	
Organization	Fine from CA Dept. of Public Health (appealed)	$250,000
Patient Services	Data for 20,000 patients posted online for nearly a year	
Patient Privacy	N/A	
Environmental	N/A	
Property, Equip, Mtls	N/A	
Labor, Time	Identity protection services provided to patients	
	This incident	$250,000
Frequency	Personal medical data for 11 million people exposed in two years (Dept. Health/Human Services)	
	Annualized Cost	?

Timeline

Date	Time	Description
1996		Health Insurance Portability and Accountability Act requires protection of medical records
September 9, 2010		Spreadsheet with patient data appears on "Student of Fortune" website
August 2011		Online company buys Student of Fortune
August 22, 2011		Breach discovered by a patient and reported to the hospital
August 23, 2011		Post removed by website
August 26, 2011		Letter sent to affected patients
?		State and Federal Agencies notified

Hospital Data Breach Exposes Medical Information for 20,000 Patients
California
September 9, 2010 - August 23, 2011

Unfortunately, privacy of health records has become an increasingly frustrating issue. The Department of Health and Human Services revealed that records for 11 million people were potentially made public for over two years. A recent medical records privacy breach has made the news for the length of time the records were publicly exposed.

A hospital in California recently notified 20,000 patients that their data had been published on a commercial website from September 9, 2010 to August 23, 2011. The published data was discovered by a patient and had been used to demonstrate the use of turning data into a bar graph. This particular data had been given to an outside contractor for billing purposes. Although it did not contain information usually used for identity theft - such as social security numbers, it did include names and diagnosis codes, meaning that extremely personal information was included.

We can examine this issue in a Cause Map, or visual root cause analysis. A Cause Map begins with the impacts to an organization's goals and uses the principles of cause-and-effect to examine the causes that contributed to these impacts. Any breach of patient privacy can be considered an impact to the patient services goals. In fact, health care organizations may choose to add a new goal category of "Patient Privacy". In addition to the impacted patient services and patient privacy goals, the hospital was fined $250,000 (the maximum) by the California Department of Public Health and provided identity protection services to the affected patients. Given the astonishingly large numbers of medical records accidentally made public, this is an issue to which all healthcare facilities should be paying attention.

The exact method that the data made it onto a public website (which provided homework assistance) is not known, but the data had been provided to an outside contractor used for billing purposes. The contractor is no longer being used by the hospital, and some privacy experts say that better confidentiality agreements are needed by hospitals who provide patient information to outside contractors. What is particularly disturbing about this case is that the data remained online for nearly a year - and was discovered by a patient. However, there does not seem to be a practical way for individual organizations to monitor the internet for misplaced patient data. Instead, focus should be on ensuring better protection upfront for medical data, in an attempt to limit breaches of patient privacy.

Step 2. Cause Map