HIPAA BREACH — Cause Map

Data from 187,533 patients compromised

"Clients entrust their information to us and we take the security of that information very seriously. We are ultimately responsible for the safekeeping of that information and regret that in this rare instance some information may have been accidentally shared inappropriately."

Cause Mapping is a Root Cause Analysis method that captures basic cause-and-effect relationships supported with evidence.

CAUSE MAPPING
Problem Solving • Incident Investigation • Root Cause Analysis

- Step 1 — Problem — What's the Problem?
- Step 2 — Analysis — Why did it happen?
- Step 3 — Solutions — What will be done?

1 Problem

What	Problem(s)	Protected health information compromised
When	Date	April 6, 2013 - Error made
		May 21, 2013 - Error corrected
		July 1, 2013 - Clients notified
	Different, unusual, unique	Customized code developed for center
Where	State, city	Indiana
	Facility, site	Family and Social Services Administration
	Unit, area, equipment	Document management system
	Task being performed	Correspondence to patients

Impact to the Goals

Patient Safety	None
Employee Impact	?
Compliance	HIPAA breach
Organization	Breach of patient trust
Patient Services	Patient confidential information compromised
	Risk for identity theft
Environmental	None

Frequency	Previous HIPAA violation in 2012 caused by theft of company laptop

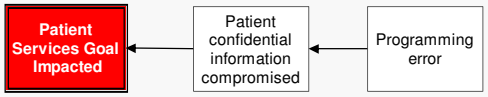
In this case, identity theft is a potential issue because of the compromised patient and financial information, especially social security numbers. The longer the period between the potential breach and when patients are notified, the greater the risk for identity theft. From the date that the programming error was incorporated into the system until the patients were notified of the breach was 86 days. 34 days elapsed before the error was noticed, but there has been no explanation for the additional 52 days before the notification.

Clients were sent confidential health and financial information belonging to other clients. An improperly used variable resulted in an error in the customized coding provided by a contractor to the agency.

The potentially compromising mailing continued for 45 days, increasing the number of people impacted. Of these 45 days, it took 34 days to notice the error. After the error was discovered, the mailings apparently continued while the error was being fixed for 11 days. This is yet another line of inquiry to be undertaken during the analysis. Ideally solutions will help to implement fixes faster - and make sure that breaches don't continue when a system is known to be working improperly.

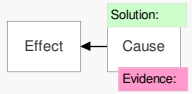
2 Analysis

Basic Level Cause Map - Start with simple Why questions.

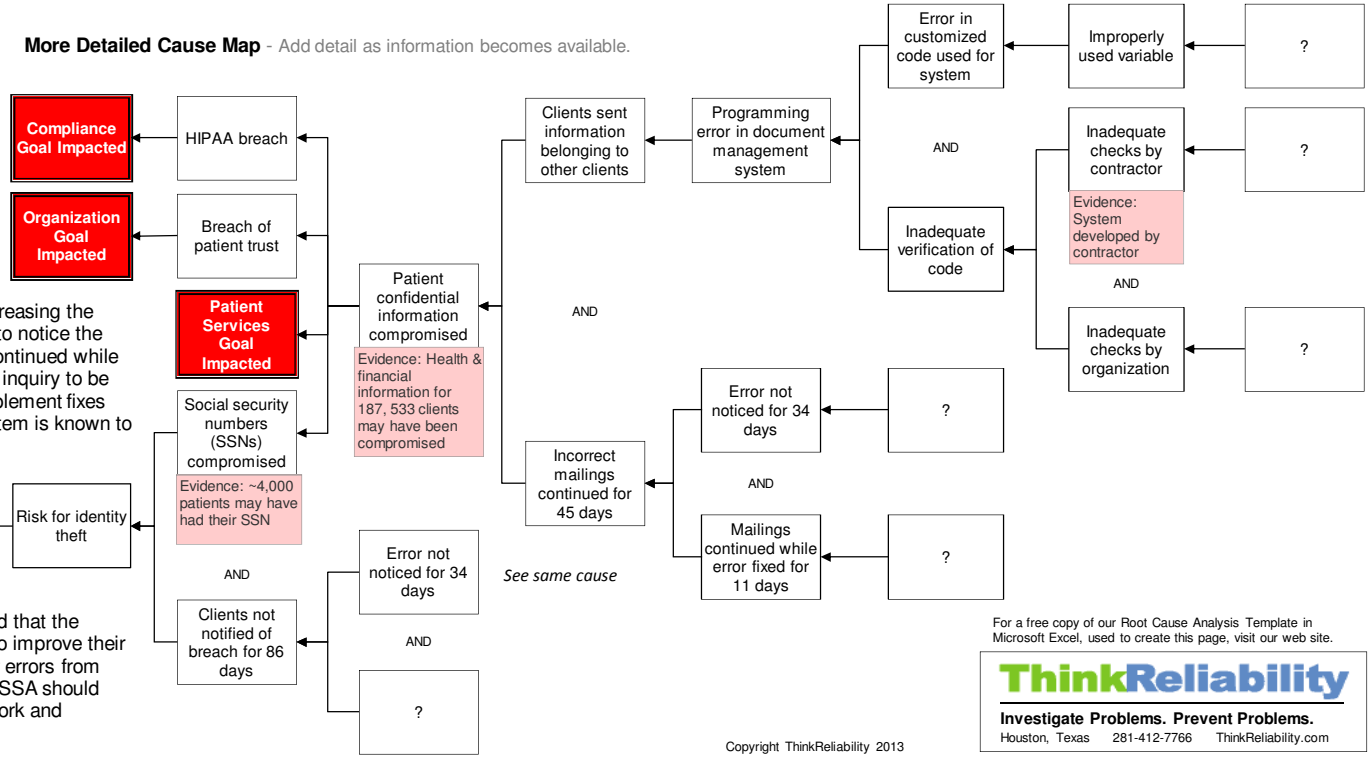


Basic Cause-and-Effect

A programming error in a document management system resulted in the data of 187,533 clients of an Indiana agency potentially being compromised. Of these, nearly 4,000 may have had their social security numbers disclosed.



More Detailed Cause Map - Add detail as information becomes available.



3 Solutions

In a letter sent to the clients potentially affected, the FSSA stated that the contractor who provides the programming "also is taking steps to improve their computer programming and testing processes to prevent similar errors from occurring in the future." While this is certainly necessary, the FSSA should also be looking at their own processes for verifying contractor work and notifying clients in the case of a data breach.

For a free copy of our Root Cause Analysis Template in Microsoft Excel, used to create this page, visit our web site.

ThinkReliability
Investigate Problems. Prevent Problems.
Houston, Texas 281-412-7766 ThinkReliability.com