# Breach Notification Laws and the American Patient

**Tyrone Grandison**

*Health Informatics, IBM Almaden Research Center, San Jose, CA*

**Abstract**

*Since California's pioneering Breath Notification Law (CA SB 1386 Senate Bill) came into effect on July 1, 2003, there has been a significant number of states that have crafted their own breach notification laws. The intent of these activities is to notify people whose information was compromised by the companies holding their data. In this work, we study the current Federal breach notification initiative and the impact on the American patient*

***Keywords:***

Privacy, Jurisprudence

## Introduction

In August of 2009, the Department of Health and Human Services issued the Breach Notification Interim Final Regulation (74 FR 42740) [1], which are regulations that implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA). The public comment phase for this regulation ends in October 2009. In this work, we explore the important tenets of this regulation and present the support healthcare information technologies and research directions that must be performed as a consequence.

## Methods

In this work, the thirty-two pages of the regulation were analyzed and the stipulations that required corresponding technological elements for support and or compliance were isolated and researched.

## Results

Based on the analysis, both a research agenda and a solutions agenda that would help healthcare practitioners meet this regulation were created. The research agenda includes work in the area of harm[1] detection, calculation and analysis and work into "technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals" [1]. In the regulation text, lots of mention is made of the latter technology and encryption and destruction technologies are the only specific examples provided. However, encryption is not a hundred secure and does not allow complete unusability, unreadability and indecipherability. Thus, this opens up new possibilities for the health informatics research community.

The solutions agenda includes notification technologies that reduce the burden on the patient. The regulation states "By imposing a duty on all covered entities to notify affected individuals of breaches of protected health information, the statute and the interim final regulation place a similar burden on all covered entities to notify affected individuals and run the same risk of losing business as a result of notification. Moreover, requiring breach notification creates an incentive on all covered entities to invest in data security improvements in efforts to minimize the possibility of reportable data breaches." [1] Commenters on the regulation also noted that notification of each and every breach that occurred would place an unfair burden on the resources of the covered entity. Both of these assertions hold significant promise for healthcare solutions vendors. There is even scope for more research in this particular area.

Other supporting technologies would be patient-centric risk dashboards that would enable analysis of a covered entity (and or business associate's) breach history and comparative analytics technologies to relative safety of one entity over another.

In this work, we also present thoughts on possible changes to the regulations to ensure that the patient is the first priority, with the covered entities and business associates in a solid secondary role. This would represent necessary shift in regulation to enable the vision of a patient-centric healthcare system in the United States of America.

## References

[1] The Department of Health and Human Services, "The Breach Notification Interim Final Regulation (74 FR 42740)". August 2009. http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

[1] Harm is used a lot in the regulation and never defined.