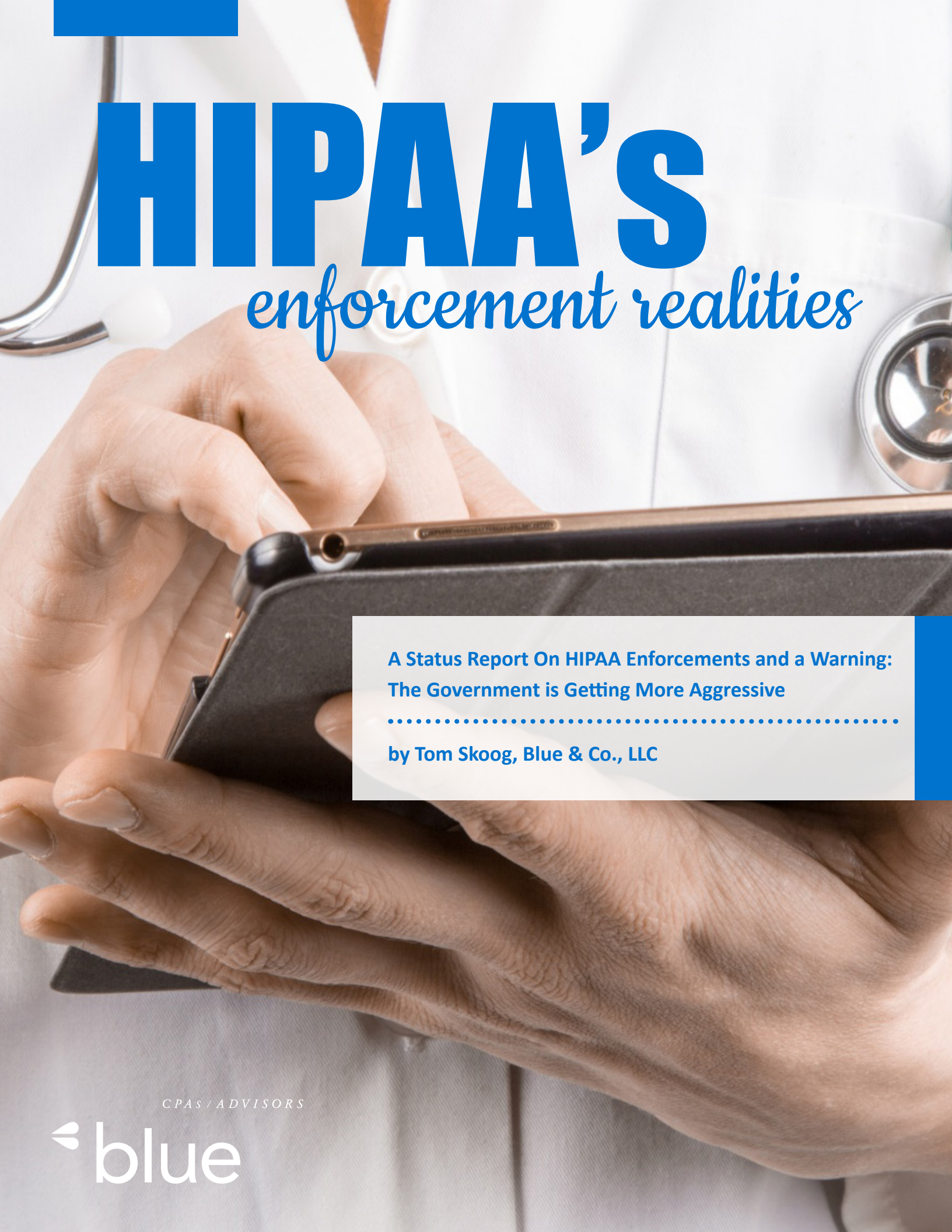
HIPAA's *enforcement realities*



A Status Report On HIPAA Enforcements and a Warning: The Government is Getting More Aggressive

by Tom Skoog, Blue & Co., LLC

CPAs / ADVISORS

blue

HIPAA's enforcement realities

A Status Report On HIPAA Enforcements and a Warning:
The Government is Getting More Aggressive

If organizations impacted by HIPAA thought the government would be relaxing a bit with a new administration, they should think again.

By the end of May 2017, The Office for Civil Rights (OCR) within Health and Human Services (HHS) had already fined nine different healthcare organizations a total of $17 million for various HIPAA compliance violations. With an average fine of $1.9 million per enforcement, 2017 is trending at a rapid rate, and will undoubtedly surpass the total fines levied in 2016. Here's a little more perspective: the fines of 2016 totaled more than $23 million. Compare that to the approximately $8 million in both 2015 and 2014, and the $3.8 million in 2013.

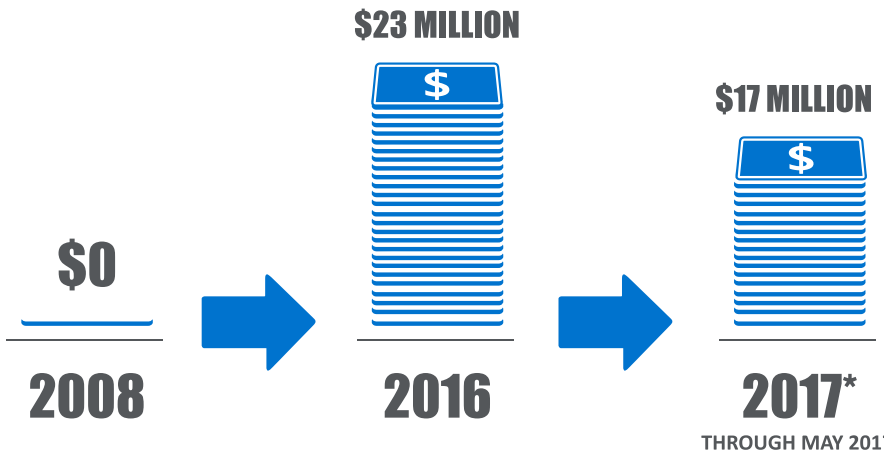
Fines are increasing at an exponential rate.

AVERAGE FINE PER ENFORCEMENT

THROUGH MAY 2017

$1.9 MILLION

FINES FOR HIPAA VIOLATIONS



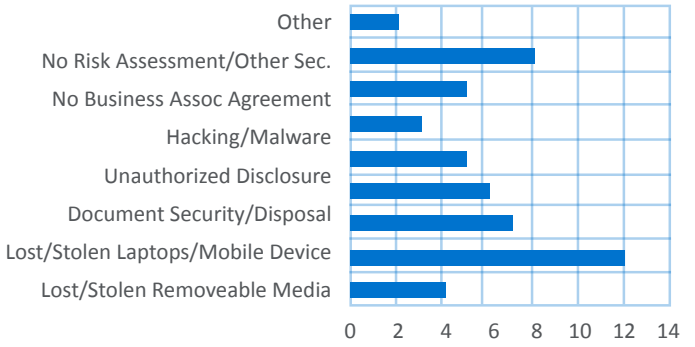
Since the passage of the HITECH Act in 2012, the number of enforcement actions taken by OCR has increased dramatically. For the five years up to, and including, 2012, OCR had a total of 12 enforcement actions with combined fines of $12 million. For the next four and a half years, 2013 - May, 2017, there have been **40** enforcement actions with fines totaling **more than $60 million – a 500% increase** between 2008 and 2012 .

CPAs / ADVISORS

blue

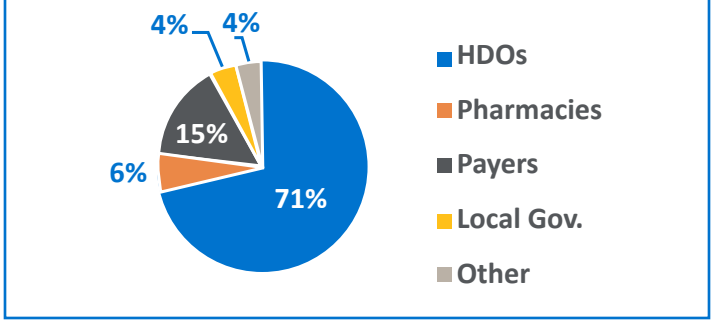
While many of these fines were levied because of self-reporting requirements included in HITECH, many others were the result of an aggressive compliance and/or investigative posture taken by OCR. In terms of self-reporting, OCR conducts thorough investigations into reported breaches, and often are citing the organizations not only for the exact cause of a breach (e.g., a stolen laptop), but also for a lack of security controls – including the lack of a detailed and robust IT security risk assessment.

HIPAA VIOLATIONS RESULTING IN ENFORCEMENTS



The reasons for the breaches are as varied as the types of organizations being fined. While stolen laptops are the leading culprit and Health Delivery Organizations (HDO) have suffered the brunt of the enforcements, no sector of the healthcare supply chain is immune. Of the 52 enforcements from 2008 to present, 37 have been brought against HDOs – including four university health systems.

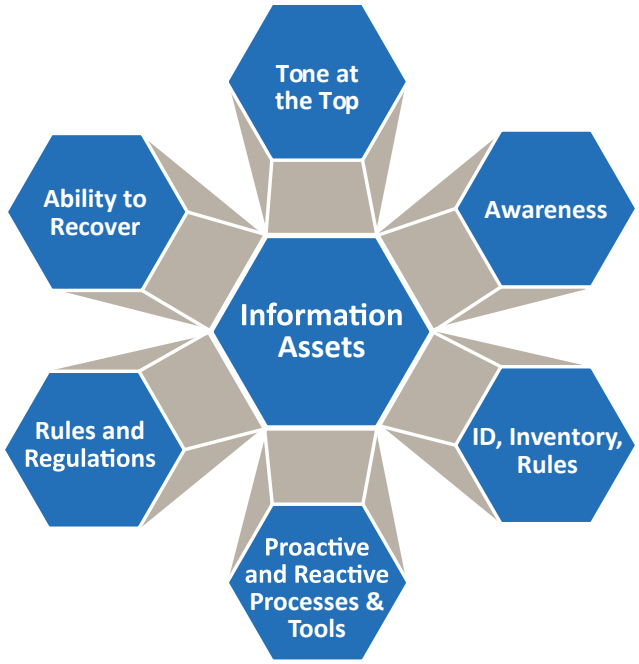
ENTITY TYPE



In addition to these enforcement actions, OCR began their second round of compliance audits of covered entities and their business associates, with announcement letters issued in July of 2016. **In this second round of audits, OCR indicated they would be focusing on smaller and medium-sized covered entities.** The purpose for this is the demonstrated difficulties these entities had with compliance during the Phase 1 audit process.

Healthcare organizations must begin addressing their security and privacy risks in a more holistic and managed measure. Between the regulatory compliance processes, coupled with the industry being targeted by more and more bad actors in the cybersphere, healthcare is at a greater financial risk than any other industry. In addition to the breach notification costs incurred (credit monitoring, etc.), healthcare gets the double financial impact of OCR fines.

As a starting point, entities must be able to demonstrate they have assessed the risk to ALL electronic protected health information (ePHI). That first involves understanding the flow and storage locations (all storage locations) of said information. From there, organizations are in a better position to ensure they are designing their controls in a way that minimizes the risk of breach and ensures compliance with the HIPAA Privacy and Security requirements and the HITECH breach notification rules.



Blue & Co. is uniquely positioned to help our clients both address the compliance requirements and enhance their overall cyber security program. Our IT Risk Management practice includes professionals with decades of cyber security experience that have worked with OCR as part of the Phase 1 audit process. Our methodology begins with understanding the value of and risk to your information assets, then we work outward on designing controls commensurate with the threats and risks to your information. We have also designed methodologies to perform your security risk assessments in the most cost-effective way possible.

If you would like to begin a discussion regarding HIPAA compliance or cyber security, please contact Tom Skoog at tskoog@blueandco.com.

CPAs / ADVISORS

blue

We are responsive. We are caring. We are advocates.

blueandco.com