



AHLA

# HEALTHCARE COMPLIANCE RESOURCE GUIDE

## SPONSORS

Booz Allen Hamilton  
Deloitte Financial Advisory Services LLP  
HORNE LLP  
Huron Consulting Group  
MedManagement, LLC  
Navigant  
Pendulum, LLC  
Pershing Yoakley & Associates  
Simione Healthcare Consultants  
Strategic Management Services LLC

© 2013 by American Health Lawyers Association

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the express written permission of the publisher. Provided, however, that this publication may be reproduced in part or in whole without permission from the publisher for non-commercial educational purposes designed to improve health in communities and increase access to healthcare or improve the quality or maintain the cost of healthcare services. Any such community benefit distribution must be without charge to recipients and must include an attribution to American Health Lawyers Association as follows:

“Copyright © 2013 by the American Health Lawyers Association and reproduced for the benefit of and to promote the health of the community served by the distributing organization.”

American Health Lawyers Association  
1620 Eye Street, NW  
6th Floor  
Washington, DC 20006  
(202) 833-1100  
[www.healthlawyers.org](http://www.healthlawyers.org)  
[www.healthlawyers.org/PublicInterest](http://www.healthlawyers.org/PublicInterest)

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.  
—From a declaration of the American Bar Association

# 2013 Healthcare Compliance Resource Guide

**Sponsored by:**

Booz Allen Hamilton

Deloitte Financial Advisory Services LLP

HORNE LLP

Huron Consulting Group

MedManagement, LLC

Navigant

Pendulum, LLC

Pershing Yoakley & Associates

Simione Healthcare Consultants

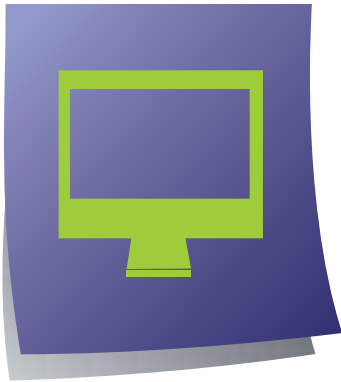
Strategic Management Services LLC

# Fraud and Compliance Forum eProgram

Purchase the Fraud and Compliance Forum eProgram and you'll be able to listen to the sessions you missed, refresh your memory of sessions attended, train associates, quickly locate and download all of the useful information and practical tools from the materials when you need them in your practice!

The eProgram contains:

- » Detailed Table of Contents
- » Complete List of All the Practice Tools and Appendix Materials (including case studies, sample forms, policies and agreements, and checklists with electronic links to each of these documents)
- » Recordings of Each Session



## What's an eProgram?

ePrograms are compressed file downloads that include a PDF of the complete program agenda, with hyperlinks to the mp3 audio files and the written materials for each of the sessions on that program.

***Special thanks to PYA for sponsoring the Fraud and Compliance Forum eProgram.***



\*The eProgram will be emailed out to purchasers approximately 6 weeks after the program ends. Once purchased, ePrograms are available in the "My Product Downloads" section of the website. Visit our bookstore at [www.healthlawyers.org/eprograms](http://www.healthlawyers.org/eprograms) to order an eProgram today!

# PREFACE


## Healthcare Compliance Experts Take the Stage in AHLA's Vendor Resource Guide!

---

### Preface

**A**s part of its ongoing coverage of healthcare compliance, AHLA is pleased to offer its business partners the opportunity to profile their expertise in this area. A number of our partners have graciously agreed to contribute to this Resource Guide and have provided AHLA with educational sponsorships to support its development. This Resource Guide contains extremely valuable analysis and commentary about current compliance issues from leading healthcare experts. We are pleased to be able to publish this collection of timely, practical, and valuable articles for the benefit of our members and the broader healthcare community.

We encourage readers to take the time to look through the *Healthcare Compliance Resource Guide* and to examine each article. The articles are all unique and each one contains pearls of valuable data and advice for all professionals who work in this area. AHLA is grateful to be able to add this new resource to its already impressive array of products and services. ALHA thanks each and every one of the sponsors of the *Healthcare Compliance Resource Guide* for making it possible.

A close-up photograph showing two hands holding two interlocking puzzle pieces. The pieces are light blue with a slightly textured surface. The background is a soft, out-of-focus light blue.

PETER M. LEIBOLD  
Executive Vice President, CEO  
American Health Lawyers Association  
[pleibold@healthlawyers.org](mailto:pleibold@healthlawyers.org)

## Corporate Compliance Across the Long Term Care Continuum Seven-Part Master Class Webinar Series

With increased government scrutiny over both payment and quality of care, it has become critical for long term care providers across the continuum to maintain a comprehensive and effective corporate compliance program. This master class series of webinars will go beyond the basics to delve into the factors that distinguish extraordinary compliance plans that work for the provider from those that sit on the shelf gathering dust. The series will focus on post-acute provider compliance generally, but will also delve into the specific issues facing skilled nursing facilities, assisted living facilities, and home health agencies.

**October 2013–April 2014**

**Part I: Corporate Compliance Basics**

Wednesday, October 2, 2013

**Part II: Implementation, Session I**

Tuesday, November 5, 2013

**Part III: Implementation, Session II**

Tuesday, December 3, 2013

**Part IV: Assessing the Effectiveness of the Compliance Program and Special Issues**

Thursday, January 23, 2014

**Part V: Skilled Nursing Facilities**

Thursday, February 6, 2014

**Part VI: Assisted Living Facilities**

Thursday, March 13, 2014

**Part VII: Home Health Agencies**

Thursday, April 24, 2014



For more detailed information about each part of this series and to register, visit [www.healthlawyers.org/LTCMasterClass](http://www.healthlawyers.org/LTCMasterClass).


All sessions will be held from 1:00-2:30 pm Eastern.

---

# Contents

<b>Partner Risk Management: Evolving Towards a More Effective and Efficient Risk-Based Approach</b> <i>Booz Allen Hamilton</i> .....	3
<b>After An Allegation: Conducting An Effective, Efficient Internal Investigation</b> <i>Deloitte Financial Advisory Services LLP</i> .....	9
<b>Privacy and Security Considerations for Cloud Computing Services</b> <i>HORNE LLP</i> .....	15
<b>Structuring An Effective And Efficient Research Compliance Program</b> <i>Huron Consulting Group</i> .....	23
<b>Establishing Processes to Document Medical Necessity: The Best Offense to Avoid Government Recoupments and Investigations</b> <i>MedManagement, LLC</i> .....	35
<b>Harnessing the Power of Data: A Primer for Health Care Attorneys</b> <i>Navigant</i> .....	39
<b>Striving for Quality and Staying in Compliance</b> <b>A Continuous Challenge for Long Term Care Facilities</b> <i>Pendulum, LLC</i> .....	45
<b>Demonstrating Compliance Program Effectiveness in an Ever-Changing Healthcare World</b> <i>Pershing Yoakley &amp; Associates</i> .....	51
<b>Achieving Quality and Compliance in Home Health and Hospice Care</b> <i>Simione Healthcare Consultants</i> .....	55
<b>Challenging Overpayment Extrapolations: Statistical Considerations</b> <i>Strategic Management Services LLC</i> .....	61





**Increased regulatory  
focus.**

**Heightened  
accountability.**

**Enhanced  
compliance.**

Are you prepared to deal with the rapid changes to managing Partner Risk in Healthcare? Former competitors have become allies in the pursuit of delivering more connected, cost effective, and high quality care. As the market continues to consolidate, how you manage Partner Risk could be the difference between thriving and falling behind. Booz Allen Hamilton can help you incorporate a new risk based and data-centric model of Partner Risk Management into your enterprise risk management and governance program. Our solutions help you maximize the effectiveness of stretched resources and directly support your organization's implementation of next generation technologies and care delivery models.

For more information on how Booz Allen can help you manage your regulatory compliance strategies, contact Bill Fox at [fox\\_william2@bah.com](mailto:fox_william2@bah.com). See our ideas in action at [boozallen.com](http://boozallen.com)

**Booz | Allen | Hamilton**  
strategy and technology consultants



# Partner Risk Management Evolving Towards a More Effective and Efficient Risk-Based Approach

*Bill Fox, Principal, Risk and Regulatory Compliance – Health Practice Lead, Booz Allen Hamilton, [fox\\_william2@bah.com](mailto:fox_william2@bah.com)*

*Albert Belman, Principal, Supplier Risk Management Practice Lead, Booz Allen Hamilton, [belman\\_albert@bah.com](mailto:belman_albert@bah.com)*

*John Binkley, Lead Associate, Risk and Regulatory Compliance – Health Practice, Booz Allen Hamilton, [binkley\\_john@bah.com](mailto:binkley_john@bah.com)*

*Phillip Sarnowski, Lead Associate, Risk and Regulatory Compliance – Health Practice, Booz Allen Hamilton, [sarnowski\\_phillip@bah.com](mailto:sarnowski_phillip@bah.com)*



## Introduction

**T**he healthcare industry is rapidly becoming more integrated. Driven by the Affordable Care Act (ACA), risk driven payment models, and financial pressures, new partnerships are forming daily – former competitors have become allies in the pursuit of delivering more connected, integrated, and longitudinal care. These new relationships are more data-centric (rather than focused on business process), and require that patient data be shared, oftentimes between diverse organizations ranging from payers to large integrated health systems to small, independent physician practices. Similarly, healthcare providers are interacting more regularly with other types of organizations not directly related to the provision of care, including health information exchanges (HIE), clinical registries, and clinical analytics firms. How well are healthcare providers evaluating the added security risks of these new partnerships? Moreover, are they re-evaluating established relationships also predicated on the exchange of Protected Health Information (PHI)?

Processes have existed for years to assess the initial and ongoing risk of partnerships (for example, questionnaires), but these established processes are not suitable for the new reality. The volume of new partnerships, the velocity with which they are being formed, and the associated business risk demand more effective and efficient Partner risk management practices. The full spectrum of these risks can include financial, compliance, business continuity, reputational, regulatory, and operational risks. Risk governance functions must adapt to address this spectrum of risk in their Partner risk management programs. Healthcare providers must be able to establish the security risk of new Partners while also evaluating and understanding the ongoing risk associated with existing partnerships.

The current trend toward integration and consolidation in the market will eventually result in a smaller number of dominant players, while others will be left behind. To survive this consolidation, organizations must move away from traditional

## Partner or Vendor?

**Vendor Risk Management is a term more suited to the older ecosystem. In the new ecosystem, data driven relationships are more complicated and interdependent, thus we use the term Partner. Vendors are an important subset of Partners, but only a subset. The term Partner is utilized wherever data travels.**

thinking that treats cost and risk as separate items. Cost and risk cannot be treated as independently set goals. Rather, to optimize for cost and risk, it must be understood that they are becoming inexorably unified. To survive and thrive in this environment, healthcare providers must adopt cost effective approaches to Partner risk management and enhance their ability to connect and collaborate with their peers in industry.

## HIPAA Omnibus Final Rule & Partner Risk Management

The Health Information Portability and Accountability Act (HIPAA) Omnibus Final Rule released in January 2013 expanded the privacy and security responsibilities of Partner organizations, thereby redefining how the health care industry views Business Associates (BA). There is now a broader population of BAs (including organizations such as health information exchanges) who now must be fully compliant with the Security Rule.

The Omnibus Rule brings major changes to the Partner organization community. Before the Final Rule, Partner organizations were only held responsible per their contractual agreements to Covered Entities (CE); they now face direct scrutiny from the Department of Health and Human Services (HHS) Office of Civil Rights (OCR), the agency charged with enforcing HIPAA. Many Partner organizations have so far resisted signing BA agreements. In fact, this has become a common complaint of CEs. Even such critical Partners as cloud computing vendors

have been resistant to signing such agreements.

The Omnibus Rule also extended BA agreements downstream to subcontractors of partner organizations. Under the new Rule, the term “subcontractor” is defined broadly enough to encompass almost anyone with access to PHI. Taken together with the new requirements for BA agreements with CEs, the Partner organization community now faces increasing business risk complexity. These organizations need to be prepared to support and defend, perhaps during an OCR audit, their compliance plan and risk management decisions.

Also, while the new HIPAA Omnibus rule does make BAs directly liable for non-compliance, the Covered Entity still must obtain assurance that the BA is protecting its PHI. The burden of patient notification, the ensuing negative publicity, and reputational damage still lies with the CE. *Reputational risk remains unchanged.* CEs must implement solutions that validate their Partners’ (i.e., BAs’) unique security postures and spell out the likelihood, risk, and impact of non-compliance.

### How is the Market Responding So Far?

In order to meet this challenge, the compliance-based “check box”/ “One size fits all” approach will have to evolve into a new approach that embraces both compliance and risk. An organization cannot be strong everywhere; it must concentrate its resources at the point of greatest risk. The multitude of organizations that you do business with do not all present the same level of risk and they must all be evaluated based on the most accurate risk picture that can be created.

On May 8, 2013, HITRUST announced that it had reached an agreement with a group that includes CVS Caremark, Health Care Services Corp., Highmark, Humana, United Health Group, and WellPoint to require all the BAs of this group to submit HITRUST Common Security Framework (CSF) assessments. This agreement is an effort to reach a critical mass of organizations that will apply a single control and reporting framework for their universe of BAs and Partner organizations. While this will be phased in over time, it could ultimately be a sea change for BAs and CEs.<sup>1</sup>

While HITRUST is taking steps to attempt to streamline Partner risk management across the health industry, CEs cannot stand by and wait for these or other arrangements to fully take effect; they must act now. Traditionally, the Partner (BA) risk picture has been driven by non-standardized questionnaires that drain significant time and resources from doing business and delivering healthcare. When a Partner receives a questionnaire, he/she is being asked to “self-attest” to its own risk issues. Regardless of the integrity of an organization, it is important to recognize that asking Partners to potentially act against their own self-interest introduces significant risk into the equation. Even the most “conscientious” Partners might have serious risk issues and weak controls, and therefore have limited understanding of their true security posture. Poor security controls often go hand-in-hand with poor governance and awareness.

### Example Potential Negative Outcomes of Breaches

- |                                    |                                      |
|------------------------------------|--------------------------------------|
| • PHI Compromise (Confidentiality) | • Intellectual Capital Compromise    |
| • PHI Compromise (Integrity)       | • Disruption of Service Availability |
| • PII Compromise                   |                                      |

In addition, questionnaires often overlook the portion of the risk picture that arises within the CE. Here, the distinction between primary and secondary controls and threats comes into play. In the same way that primary controls are based on your Partner’s direct actions and secondary controls involve areas that can be addressed internally to enhance your Partner’s primary controls, a risk score can be based on primary and secondary factors. While you may have concerns about determining how your Partners handle risk (primary factors), a significant number of variables that go into the risk equation come from within (secondary factors), such as the amount of data that Partners have access to and how they access the data. Therefore, you can build an initial risk score utilizing information assembled within your own organization, and do not have to solely rely on the self-attestations of another organization. Understanding the amount and nature of a Partner’s access to your systems is the first step in understanding the risk they present to your organization.

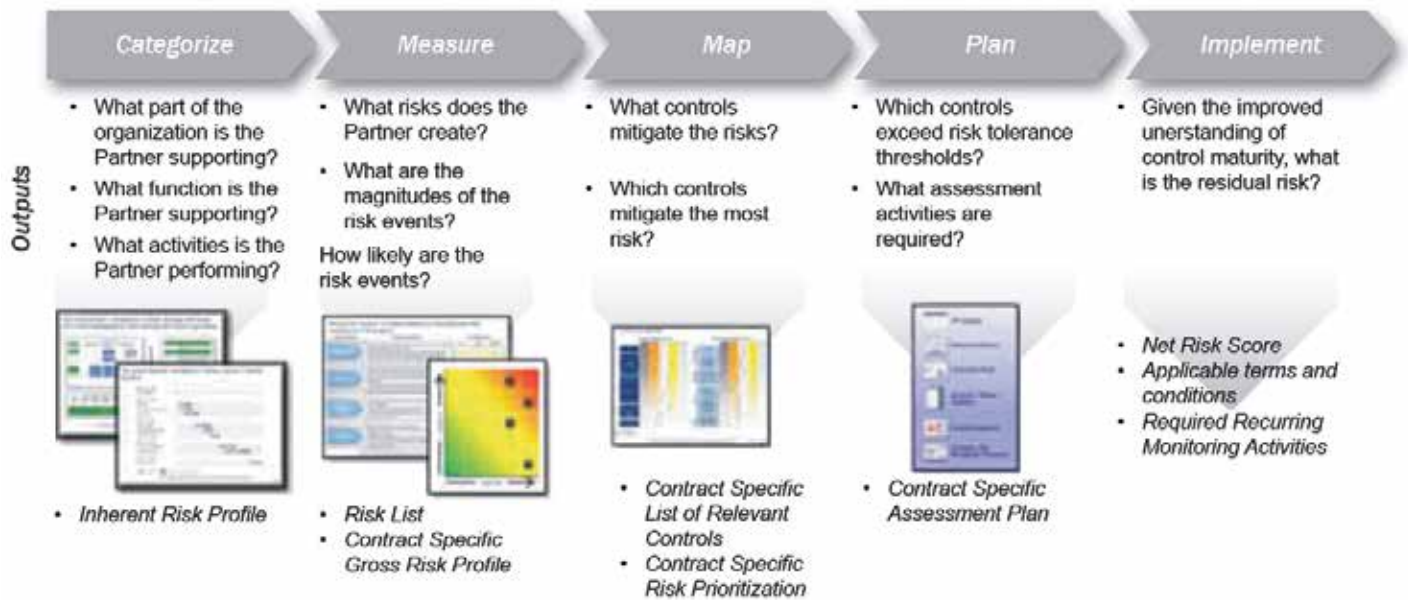
### How Should Covered Entities Evaluate Partner Risk?

Applying effective risk management capabilities, such as assigning initial risk scores, can allow CEs to effectively evaluate Partner risk while still maintaining compliance. To do this, a CE needs to focus on the following three principles:

1. Create a risk assessment mechanism that identifies the true, high risk partnerships.
2. Develop a continuous monitoring mechanism to identify, prioritize, and remediate or accept risks and issues throughout the life of the contract.
3. Rationalize assessment spending to risk level, avoiding wasted efforts and improving overall ROI.

This is, of course, more easily said than done. As information sharing continues to proliferate across the healthcare industry, your security posture will be increasingly dynamic and fluidly tied to the security posture of your Partners. They will have access to your sensitive data and your operations will be reliant on the services they provide. To create an assessment mechanism to identify true high risk partnerships, what is needed is a method for determining the risks for each Partner that is rapid and data-centric. Furthermore, the process must be designed so that non-technical staff routinely involved in contractual issues can

<sup>1</sup> Booz Allen has been recognized by HITRUST as a CSF assessor.



determine the initial score. The Booz Allen model uses a specific Partner Risk Scoring Model.

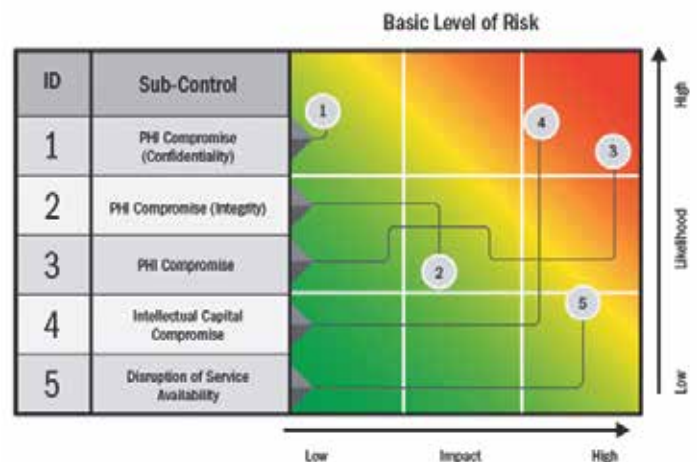
Healthcare is becoming more data-centric, and thus, so are its risk calculations. Other industries require partnerships, but rarely do those partnerships require you to share the proverbial “crown jewels” in terms of data sets. Other industries tend to be more focused on business processes and less on sharing such critically private and regulated information. You will need to know the quality and quantity of information to which a prospective Partner will have access. What types of data (for example, PHI, PII, intellectual capital) will a Partner be able to access? If it is PHI, how many records will be at risk? How will Partners access this information?

Here, we must utilize the concept of “quick” look and “long” look. A “quick look” initial evaluation of risk must be performed rapidly with a limited information set, and by people who may not necessarily be fully versed in compliance and security. The advantage that you do have is that within most health sector organizations, almost everyone understands at least the broad strokes of identifying PHI. There are techniques and risk models that can be utilized to refine the process, but the results will be a rough order-of-magnitude initial risk score.

These outcomes, when coupled with some simple contextual questions, will allow you to establish an initial risk score for a particular Partner. This initial score is by no means intended to be the final word on the subject. Rather, this score serves as a trip wire to help you determine exactly what “long look” assessment tools are necessary to more accurately judge the risks presented by a specific Partner. Depending on the risk score, a different, more involved tool might be required. Booz Allen has developed models that can provide risk scores and guidance on specific security and compliance control families. The more risk posed by the Partner, the more involved assessment tool is needed. For Partners with high risk, enhanced risk assessment procedures may be appropriate. These enhanced assessments should be deeper, longer looks, but also focus on the specific areas of concern.

There are different stages to this process. You must ensure that the correct “long look” assessment or risk mitigation activity is appropriate to the different types of partnerships. What is suitable for one type of Partner might not apply to another. Using these means, organizations can quickly generate a picture of security-related risks amongst their community of Partners. This type of analysis can guide the efforts of compliance and information security teams and help determine how resources should be allocated.

This addresses the first of the three principles cited previously for establishing a risk assessment mechanism. To be truly effective, the process must also address a way to continuously monitor the risks associated with each Partner. These are not one-time activities. “Quick look” assessments should be conducted to monitor each data sharing connection and ensure that the appropriate level of risk is assigned. Many events can change the nature of a risk assessment; a Partner’s status may change, a regulatory rule might be interpreted differently, or new attack vectors might be brought into play. To leverage the utility of an accurate risk assessment, you must be able to monitor the risk over time.





Assessing and monitoring risk is a means to an end. The end goal is to be able to rationalize the expenses associated with securing Partner risk. Managing Partner risk effectively in this environment is about speed, flexibility, managing ambiguity, and using the most complete risk picture you can build to marshal your resources where they are most needed. A good Partner risk management program focuses precious resources where they are most needed. In managing Partner risk, you will be held accountable for the company you keep - make sure you have a true understanding of the risks involved and choose wisely.

## Conclusion

Some organizations think of risk management and compliance as two different things. Booz Allen considers risk and compliance to be intertwined and finds that this integrated view brings value and efficiencies to the process. Non-compliance needs to be thought of as a risk – not the only one, by any means, but for the purposes of the Partner community preparing to follow the HIPAA Omnibus rule changes, an extremely important one.

Partner risk management is undergoing changes in the health field. Some of these changes are driven by external causes, namely the HIPAA Omnibus Rule, and some are driven by internal factors, such as the need to reduce risks while holding the line on operational costs. While these changes will be far reaching, we are not on the precipice of a revolution. Instead, the changes will be evolutionary and favor organizations that can recognize and act on the data-centric nature of the modern Partner relationship as part of a systemic risk management and governance program.

To capitalize on this moment, you will need to be able to apply a risk framework that encompasses external and internal threat factors built around specific data types and the nature of each partnership, or consult with someone who can. Only with this level of situational awareness can your organization address compliance while also applying a granular and appropriate level of risk management to each Partner activity. This approach will maximize the effectiveness of available resources and directly support your organization's implementation of next generation technologies and care delivery models. ♦

**September 29-  
October 1, 2013**  
Hilton Hotel  
Baltimore, MD

**Deloitte.**

HealthCare Appraisers  
INCORPORATED

# FRAUD & COMPLIANCE FORUM

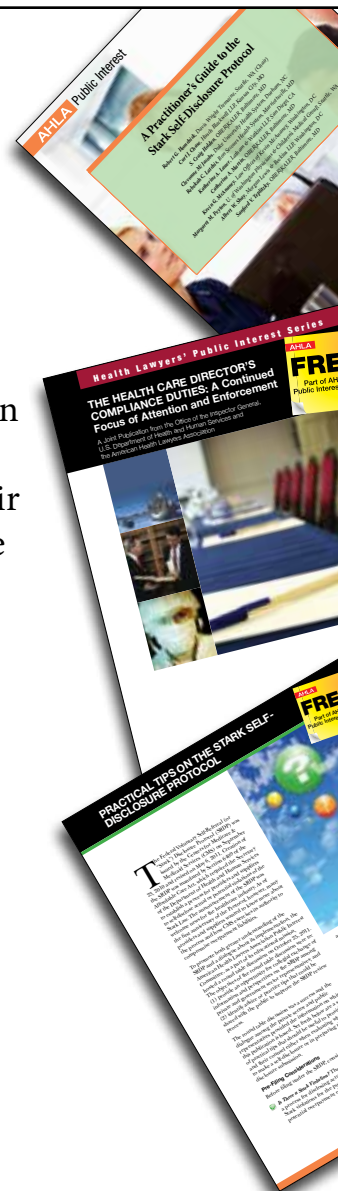
*Co-sponsored with AHLA and HCCA*

**A**HLA's Public Interest Series Healthcare Executive Collection offers free resources for hospital executives and administrators, chief compliance officers, hospital communications and community relations managers, and healthcare counsel. The collection of in-depth guidebooks, checklists, and fact sheets are prepared by AHLA members who bring unparalleled expertise and passion to their work and an enthusiasm to share their knowledge with the healthcare provider community and the general public.

## The Healthcare Executive Collection includes:

- » The Health Care Director's Compliance Duties: A Continued Focus of Attention and Enforcement
- » Practitioner's Guide to the Stark Self-Disclosure Protocol
- » Practical Tips on the Stark Self-Referral Disclosure Protocol
- » Considerations in the Disclosure of Serious Clinical Adverse Events
- » Revisiting Your Hospital's Visitation Policy
- » Emergency Preparedness Response & Recovery Checklist: Beyond the Emergency Management Plan
- » Lessons Learned from the Gulf Coast Hurricanes
- » Community Pan-Flu Preparedness: A Checklist of Key Legal Issues for Healthcare Providers
- » Community Benefit Toolkit
- » Minimizing EHR-Related Serious Safety Events

**Visit [www.healthlawyers.org/publicinterest](http://www.healthlawyers.org/publicinterest) to download your free resources.**





# Is your health care company or client...

- Under investigation?
- Evaluating various business opportunities and options?
- Buying or selling a business?
- In a business dispute?
- Involved in a plant expansion?
- In need of regulatory compliance assistance?
- In financial distress?

**Let Deloitte help you resolve your issue.**

**[www.deloitte.com](http://www.deloitte.com)**

As used in this document, "Deloitte" means Deloitte LLP and its subsidiaries. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2013 Deloitte Development LLC. All rights reserved.  
Member of Deloitte Touche Tohmatsu Limited



# After An Allegation: Conducting An Effective, Efficient Internal Investigation

**Rob Cepielik**, Partner of Deloitte Financial Advisory Services LLP  
[rcepielik@deloitte.com](mailto:rcepielik@deloitte.com)

**Mike Little**, Senior Manager, Deloitte Financial Advisory Services LLP  
[mlittle@deloitte.com](mailto:mlittle@deloitte.com)

**Greg Garrison**, Senior Associate, Deloitte Financial Advisory Services LLP  
[ggarrison@deloitte.com](mailto:ggarrison@deloitte.com)



## Introduction

**A**mong the responsibilities of a healthcare entity's compliance officer are to ensure that the organization operates in an ethical fashion and complies with all regulatory obligations. Many laws and regulations, such as Sarbanes Oxley, the Federal Sentencing Guidelines, the Securities and Exchange Commission guidelines, require that management establish a mechanism to receive confidential and/or anonymous reports from concerned employees and other stakeholders, and to protect those "whistleblowers" from retaliation.

The current regulatory and enforcement environment has raised the stakes even higher for health care providers and payers. The Patient Protection and Affordable Care Act (PPACA) introduced new obligations regarding the effectiveness of an organization's compliance program, as well as accelerated self-reporting requirements. For example, one provision mandates that a provider return any identified Medicare or Medicaid program overpayment within 60 days, with an explanation of the overpayment(s). Failure to do so renders the overpayment a false claim that could be subject to the federal False Claims Act and whistleblower provisions.

When information about an alleged impropriety comes to the attention of a health care provider's and/or payer's compliance officer (or department), it is important that the organization take appropriate and timely steps to analyze and investigate the situation, especially because it later may be required to demonstrate what actions it took in response to a complaint. As a compliance professional, you will often be asked to play an important role in an internal investigation. This article describes the anatomy of an investigation and cites leading practices that may benefit health care organizations in their investigative efforts.

- » When assessing the validity of an allegation, identify the issue as precisely as possible.
- » Decide early on the composition of the investigation team.

- » The initial investigative plan should include parameters for assembling, analyzing, and safeguarding documents.
- » Follow procedural guidelines when conducting interviews with witnesses and subjects.
- » Document an analysis of the findings and the actions that were taken at the conclusion of the investigation.

## Assessing An Allegation

When assessing the validity of an allegation, it is important to break it down and identify the issue as precisely as possible. Use the information that is available—whether from a hotline report (anonymous or named) or from internal data analysis—to ascertain whether the specific problem/complaint involves billing to government or commercial entities, financial reporting, contractual relationships with outside entities, or ethical lapses by employees or contractors.

Begin by identifying who has information relevant to the issue and where that information resides. Also assess whether there is a logical set of individuals who should be interviewed. Consider what resources will be needed to conduct the investigation, where those resources reside—both within and outside the organization—and how those resources can be obtained. Based on the information available up to this point, set a reasonable timeframe to conduct the investigation and consider the possible outcomes. Such consideration is important, because a self-disclosure to a government agency or a referral of potential criminal conduct by an employee or contractor to a law enforcement agency may significantly impact the investigation's urgency.

In conjunction with the above, a major consideration when embarking on an internal investigation is whether the investigation will be conducted under the direction of counsel. In most cases, the answer will be yes. This is especially true if the

complaint, on its surface, seems to indicate a pattern of conduct that could result in potential overpayments to the government or a commercial entity, or indicates potential criminal behavior by an employee or contractor. Counsel's involvement at the earliest stage in the investigative process is critical and provides a number of benefits. In general, when working under the direction or supervision of counsel, communications and work product will be protected under the attorney-client privilege and work product doctrine. It is important to note that such protection has limits—state laws differ, and court decisions may change interpretations. Therefore, it is advisable that the investigative team be briefed by counsel at the onset.

Another early decision that should be made is whether in-house counsel should lead the investigation or if external counsel should be retained. This decision should be based on the nature and scope of the complaint and be made in consultation with in-house counsel and, potentially, senior management and the audit committee. Strive to avoid mistakes commonly made during an initial assessment—these include underestimating the allegation, not considering the full impact of the information received, and undervaluing the credibility of an information source.

Taken together, the components of the initial assessment will provide the platform for development of an investigative plan. The purpose of this plan is to provide a roadmap to resolving the issue expediently and with assurance that all appropriate avenues are explored while avoiding unnecessary blind alleys. In short, an initial assessment helps identify the “who, what, when, where, why, and how” of the issue at hand.

## Composing the Investigative Team

After completing the initial assessment and making preliminary contact with the complainant (if that is possible or deemed appropriate), the compliance officer—in consultation with counsel (in-house or outside)—should determine the composition of the investigative team. The three most important considerations are:

- » **Discretion:** The need for discretion is paramount. An investigation should be conducted with a minimum number of individuals privy to the details. Inappropriate disclosure could exacerbate the situation or compromise the integrity of investigative process. Only those individuals who understand this should be brought into the core team.
- » **Capability:** Depending on the nature of the allegations, the investigative team should be composed of individuals with capabilities and experience in conducting competent interviews. Skill sets of team members could include clinical and/or coding credentials, forensic accounting, data analysis, and computer forensics, among others.
- » **Credibility:** The investigative team must have credibility to withstand scrutiny from within the organization and from outside parties, including government regulatory agencies, the public, and investors. Often

this credibility can be enhanced by bringing in outside resources, be they legal counsel and/or forensic accountants and investigators. The inclusion of outside resources is further indication that the organization takes the issue seriously and that the review will be competent, unbiased, and independent.

Another important item for consideration is the investigation's governance. Specifically, the roles of management and the audit committee should be agreed upon at the investigation's inception and modified as facts and circumstances emerge. As a “rule of thumb,” many believe that the audit committee should take an active role in an investigation's governance when allegations relate to accounting or financial reporting and evidence suggests that those allegations could be material; allegations could have a significant impact on the reputation of the company, including allegations of illegal acts; or allegations involving senior management of the company.

## Conducting the Investigation

A thorough investigation begins with the iterative process of developing, assessing, and reworking a plan. Typically, the investigation team will assess the original plan and re-direct efforts as necessary; specifically, it will assist in deciding what documents and records need to be assembled and analyzed, which individuals should be interviewed, and the appropriate interview sequence.

### Assembling the Documents

During the document assembly phase of an investigation, it is imperative to maintain data integrity and a clear chain of custody, because it is virtually impossible to determine what an investigation's outcome might be and what documents could be significant. Required documents that are in hard-copy form should be obtained from their custodian with clear documentation of when they were obtained, from whom, and by whom. If the documents need to be retained by the investigative team, they should be kept in a secured location with limited and documented access.

Electronic records should be obtained from their custodian and provided in a format and media that protects and ensures data integrity. As is the case for hard copies, electronic documents should be maintained in a secure, limited-access environment.

As documents (hard copy or electronic) are assembled, a critical concept is “chain of custody.” Chain of custody requires ensuring that the receipt of each document is memorialized and that a document is prepared and retained to show who originally provided the document, where it is stored, and who has had access to it.

### Analyzing the Documents

In a typical health care setting, required investigative documents will be in one of three general categories:

- » **Financial records**, which include, but are not limited to, financial statements; supporting ledgers, including general, accounts payable, accounts receivable, sales, payroll, etc.; supporting payment information,

including invoices, cancelled checks, and remittance advices; personnel records; and fixed asset and depreciation listings.

» **Contractual records**, which include contracts, mortgages, deeds, proposals, rental agreements, service agreements and subcontractor agreements. Also included could be records related to any grants received from government sources.

» **Billing and medical records**, which include, but are not limited to, physicians' orders, intake documents, treatment notes, progress notes, and billing documents such as UB04s (CMS Form 1450), detailed hospital bill/statement, etc.

The relevant documents may be analyzed in a number of ways. They may be compared to other documents (e.g., comparing medical records with claims data), or they may be used during interviews. Whatever their use, all documents should be maintained with a proper chain of custody or sourcing. Also, be particularly careful if medical records are used: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains provisions restricting the use and disclosure of documents containing protected health information.

## Interviews

Documents can tell part of the story but are lifeless; witnesses can tell part of the story and give life to the documents. Interviews may be the most significant part of a forensic investigation. Witnesses can refute allegations by providing logical explanations of things that appeared improper but, in reality, were not; conversely, they may verify and give credence to the allegations. There are several types of interviews, as well as suggestions for conducting them. First, the interview types.

### » Complainant Interview

If the investigation is the result of a complaint by a named (known) individual, interviewing that individual could be a significant start to the investigative process. That person should be interviewed as soon as possible to assure that the freshest information is available and that the organization's intent to fully and objectively investigate their complaint is communicated. Be aware that the person might go outside the organization to file their complaint if they do not think that a fair investigation will be conducted. Also, do not assume anything with respect to the complainant; it is often easy to over- or under-estimate the information provided by an employee, based on their position or prior contacts.

### » Witness Interview

There are likely to be individuals, both within and outside the entity, who could have information relevant to the issue under investigation, but who are not considered to be subjects (i.e., involved in a culpable

way if the complaint is accurate). These can be key interviews, because the individual may provide information that could explain, mitigate, or confirm the facts surrounding the complaint.

### » Subject Interview

There might be one or more individuals, identified at any stage of the investigation, who are considered to be subjects; that is, they are believed to be culpably involved in the issues of the investigation. This interview could resolve the investigative issues one way or the other. The subject might provide logical information that negates the complaint or might make admissions against their interest.

## Procedural Guidelines

Alternatively, the subject might purposefully misstate answers, be evasive, or completely refuse to answer questions. The following procedural guidelines apply to all three types of interviews, although the significance of the interview determines the level of the adherence to each.

» **Have an attorney present**—This may help keep the investigation under privilege to the greatest extent possible. An attorney's presence may also facilitate resolution of legal issues that could arise during the interview.

» **Prepare for the interview**—Interviews, especially those considered significant, should never be conducted on an ad hoc basis or without careful planning. Preparation should include the complete review of documents to be discussed and the development of detailed questions (and potential follow-up questions) based on information known to date.

» **Select the proper setting**—In general, the interview location's size and space should be conducive to note-taking, document review, and accommodating the number of participants. A private setting is preferred— one that does not allow passersby to enter or see into the room. Under some circumstances, it may be appropriate to conduct the interview off-site.

» **Select an appropriate time**—The interview should be scheduled based on its nature and the needs of the investigation. For example, if an interview is expected to be lengthy, it should not be scheduled so late in the day that it could be short cut if one of the participants needs to leave.

» **Have a witness present**—Most interviews should be conducted with an interviewer and a witness present. This is especially true for interviews with significant witnesses and potential subjects. Having two individuals conducting the interview allows one person to ask questions and the other to take notes (see below).

» **Take notes**—All interviews should be documented, and notes should be taken contemporaneously and retained.

» **Interview one person at a time**—To the extent possible, the investigative team should interview one person at a time. If two people are interviewed together, one's answer might sway or suggest answers for the other. It also can be difficult to document which person provided what answer.

## Concluding the Investigation

When all the documents have been reviewed, all individuals interviewed, and all leads followed to their logical end, a picture of the results will develop. The allegations may be substantiated, in whole or in part; or they may be refuted, in whole or in part.

Regardless of the outcome, the final phase, concluding the investigation, is as crucial as those preceding it: The results must be communicated in the appropriate way—either written or verbally—to the key stakeholders. These stakeholders may include company management (Note: if any of the management team has been implicated in the findings, discretion must be exercised); the audit committee (especially if the allegations are significant or if the findings implicate a systematic failure or potential criminal violations); independent auditors (if allegations involve the integrity of financial statements, illegal acts, or the integrity of management); and law enforcement and regulatory agencies (if the investigation has disclosed instances of false billing to the government, any potentially criminal actions, or other circumstances).

## Reporting

The selection of a written or verbal report of the investigation and its results will vary by situation. Of course, the investigative efforts' outputs—interview summaries and document analyses—are memorialized as the investigation progresses and need to be maintained. Selecting the format for the final report is best done in consultation with counsel and is typically based upon the investigation's outcome. Whether presented in written form or orally, the report should:

- » Explain how and when the investigation was initiated. Chronicle the events leading to the investigation, including the allegation and source.
- » Describe the procedures performed. Include a synopsis of the information obtained during the interviews and the review and analysis of documents/information obtained from other sources.
- » Present only factual findings. The use of subjective words should be avoided, as should conclusions that have not been established during the investigation.
- » Include potential remedial actions. These could include a self-disclosure to a payer; referral of information to a law enforcement or regulatory agency; or a referral to the Human Resources department for further action.

## Final Thoughts

Use of the following leading practices may assist health care organizations in conducting an efficient and effective forensic investigation.

1. **Focus the investigation.** Analyze the allegations, develop a plan, gather relevant data, interview appropriate individuals, and periodically re-assess and realign procedures to keep the team focused on the issues at hand.
2. **Engage in frequent communication with counsel** (internal and/or external), because it can assist the investigative team in navigating the legal intricacies that it may face. If forensic accountants and consultants are retained, communicate frequently and openly to ensure that expectations are met and the investigation is done in a complete, thorough, and efficient manner. Similarly, periodically update the independent auditing firm.
3. **Do not make assumptions or leap to conclusions;** rather, rely on information that has been analyzed and verified. This is true at every stage of the investigation.
4. **Carefully document the investigative findings** to demonstrate the actions taken. The investigative record will illustrate that the organization took proper action based upon the information available at the time. It will also show that the entity responded appropriately, if it is questioned by the government or is subjected to litigation.
5. **Make a timely decision to self-disclose or refer information** to appropriate authorities, if the investigation's findings warrant it.

Remember that each allegation and its resulting investigation are unique. Some may not require a lengthy, full-scale investigation; others may take considerable time and resources to resolve. Approaching each situation systematically can better enable health care compliance officers and their team to conduct investigations that are able to meet regulatory obligations and stand up to internal and external scrutiny. ♦

*This article, published in the July 2013 issue of Compliance Today, appears here with permission from the Health Care Compliance Association. Call HCCA at 888-580-8373 with reprint requests.*





## 2013 Healthcare Fraud and Abuse Bootcamp Webinar Series Recordings

Do you have lots of fraud and abuse-related questions and are not sure where to start? Are you an in-house counsel working in the healthcare industry, general healthcare practitioner, general litigator, government enforcement practitioner, or fraud and abuse practitioner? Purchase recordings and materials from one or all of the sessions of the six-part 2013 Healthcare Fraud and Abuse Bootcamp Webinar Series (each session lasted 90 minutes).

### February–July 2013

**Part I: Fraud, Abuse, and Waste—A Primer**  
February 13, 2013

**Part II: Stark Law**  
March 13, 2013

**Part III: Federal Anti-Kickback Statute**  
April 10, 2013

**Part IV: False Claims Act**  
May 8, 2013

**Part V: Compliance**  
June 5, 2013

**Part VI: Trends in Government Enforcement**  
July 17, 2013

For general overview and detailed information about each session, and to purchase a recording, visit [www.healthlawyers.org/13FraudBootcamp](http://www.healthlawyers.org/13FraudBootcamp).

---

Once purchased, the recordings and materials (ZIP file) are available for instant access and download in the “Electronic Product Downloads” section of your AHLA account. To access the recordings, please log in at [www.healthlawyers.org](http://www.healthlawyers.org) and click on the “Electronic Product Downloads” link located under the welcome message.





HEALTH CARE REFORM  
DECLINING TOP LINE REVENUE  
DELIVERY MODEL CHANGES  
PHYSICIAN COMPENSATION RISKS

**EVERY DAY IS A CHALLENGE**

**IN THE WORLD OF HEALTH CARE**

Since 1962, HORNE has been a trusted advisor and business partner to health care organizations across the country, delivering customized business strategies to solve today's problems while looking to the future. HORNE built its foundation in health care, and today we're one of the largest firms dedicated to your industry. **At HORNE, we're more than an accounting firm — we know the business of health care.**

Visit us at [www.horne-llp.com](http://www.horne-llp.com) to meet members of our health care team and discover more about our comprehensive services for hospitals, health systems and physician practices.



**HORNE**

CPAs & Business Advisors

[www.horne-llp.com](http://www.horne-llp.com)

© 2013 HORNE LLP

# Privacy and Security Considerations for Cloud Computing Services



*Tony Brooks, Partner and Director of IT Assurance and Risk Services  
HORNE LLP, [tony.brooks@horne-llp.com](mailto:tony.brooks@horne-llp.com)*

## Introduction

The technology world today abounds with the promotion and discussion of cloud computing services.<sup>1</sup> This is especially true in healthcare as cloud computing experiences increasing adoption, spurred by federal incentives to implement electronic health records and burgeoning demand from health care practitioners and patients for anytime, anywhere access to medical information.<sup>2</sup> Whether it be an electronic health record, scheduling, billing, medical imaging, messaging, collaboration, telemedicine, educational, or other service, cloud computing is changing the landscape of healthcare.<sup>3</sup>

Like their meteorological namesake, technology “clouds” can bring both benefits and dangers. Those who have adopted cloud computing services see numerous benefits: faster implementation, lower capital investment, knowledgeable support, mobile access, and enhanced disaster recovery, to name a few. Those taking a slower road to adoption find themselves concerned about issues such as price creep, communications bandwidth, customization, integration to legacy systems, security, and lack of operational transparency.

Although many users give cloud service providers (CSPs) high marks on security, many non-users are reluctant to adopt

cloud computing services because of privacy and security concerns.<sup>4</sup> While this concern is not unique to cloud computing (it also exists in self-hosted computing environments), it is elevated in many cases due to a lack of understanding regarding the nature of cloud computing and a lack of visibility regarding the administrative, technical, and physical safeguards deployed by the CSPs. Although a business associate agreement indicates a commitment to protect confidential patient information, it does not provide the level of assurance that healthcare organizations should require. So then, what should a user of cloud computing services do to ensure that the confidential information entrusted to the CSP is appropriately safeguarded?

## What Is Cloud Computing?

The first step is to understand cloud computing and the specifics surrounding the type of services being provided. Cloud computing has been defined by the National Institute of Standards and Technology (NIST) as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”<sup>5</sup> The NIST definition further states that cloud computing has five essential characteristics, three service models,

<sup>1</sup> *Future of Cloud Computing, 3rd Annual Survey 2013*, available at <http://northbridge.com/2013-cloud-computing-survey>.

<sup>2</sup> *Cloud Computing Health Care Market Worth \$5 Billion*, CloudTimes (July 18, 2012), available at <http://cloudtimes.org/2012/07/18/cloud-health-care-market/>.

<sup>3</sup> *Navigating the Cloud, An e-Supplement to Healthcare IT News and Government Health IT*, Health IT News (November 2012), available at <http://www.healthcareit-news.com/navigating-the-cloud>.

<sup>4</sup> *Health Care Providers Give Cloud Vendors High Marks on Security*, KLAS Research (March 5, 2013), available at <http://www.klasresearch.com/News/Press-Room/2013/cloud>; *CDW 2013 State of the Cloud Report*, available at <http://www.cdwnewsroom.com/2013-state-of-the-cloud-report/>; *Security of Cloud Computing Users Study 2013*, Ponemon Institute (March 1, 2013), available at <https://www.ca.com/us/register/forms/collateral/ponemon-institute-security-of-cloud-computing-users-study-2013.aspx>; *2012 HIMSS Analytics Report: Security of Patient Data*, HIMSS Analytics (April 2012), available at <http://www.himssanalytics.org/research/AssetDetail.aspx?pubid=79879&tid=4>.

<sup>5</sup> *NIST Special Publication 800-145, The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, U.S. Department of Commerce (September 2011), available at <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

and four deployment models.<sup>6</sup> The essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.<sup>7</sup> The service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).<sup>8</sup> The four deployment models are private cloud, community cloud, public cloud, and hybrid cloud.<sup>9</sup>

As can be seen from these definitions, the technical aspects of cloud computing can be complex and confusing, especially to someone without extensive information technology (IT) knowledge and experience. A good working definition for non-IT persons is that cloud computing is an information technology service that allows an organization to gain access to computing software, hardware and network systems on a pay-as-you-go, build-it-as-you-need-it basis with the responsibility for deployment, operation, maintenance, and support assumed partially or entirely by a third-party service provider.

### Important Privacy and Security Considerations

Regardless of the form and substance of the cloud computing services being used, is vitally important to understand the specifics of what is being provided, the administrative, technical and physical safeguards that are in place, and the delegation of responsibilities between the CSP and the organization. A simple checklist of items to consider can easily exceed 150 or more items and include areas such as logical and physical access, change management, privacy and security, environmental protection, remote and mobile access, data backup and retention, disaster recovery and business continuity, regulatory compliance, e-discovery, maintenance, support, training, performance, and availability. Since privacy and security is a chief concern regardless of how cloud computing services are deployed, let's look at several important areas that should be considered. Remember, these areas are equally as important in a self-hosted computing environment.

#### Regulatory Compliance

The Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act, and the Omnibus Final Rule provide a set of national standards requiring the protection of certain health information in both electronic and non-electronic form.<sup>10</sup> Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted data breach notification legislation that applies when a breach of certain personally identifiable information occurs.<sup>11</sup> Some states have stricter

requirements than HIPAA/HITECH/OMNIBUS, thus complicating compliance. Healthcare organizations must ensure that they and their CSPs understand these and other privacy and security requirements and have policies and procedures in place to not only ensure the confidentiality, integrity, and availability of protected health information (PHI), but to ensure that breach notification responsibilities are clearly described and assigned.

#### Location

It may be surprising to learn that many organizations that use cloud computing services do not know where their data is physically located. In fact, CSPs may not know at a specific point in time where all of a customer's data is located. This uncertainty is a result of the widespread use of virtual server software, which allows a single hardware server to host one or more virtual servers that can be automatically or manually moved or reconfigured in a short period of time. It is also a result of the pervasive use of data storage systems that replicate data for disaster recovery purposes frequently, and in some cases in nearly real time, to storage systems and removable storage media in other locations. Similarly, data may be stored in different development, test, and training systems outside the production environment. As a result, software application systems and related data can exist in whole or in part on multiple servers, data storage systems, and storage media located in more than one facility, in some cases several states away or in other countries.<sup>12</sup> While internal controls may be in place to protect this information and even restrict its movement outside specified geographic regions, it is very important to understand how application systems and data are being processed, stored, and replicated so that an organization can assure that protected health information is adequately safeguarded, that regulatory and contractual requirements are met, and that legal and other risks related to systems and data location are fully addressed.

#### Virtualization and Multi-Tenancy

One of the key benefits of cloud computing is economy of scale and the related cost savings. This benefit is the result of the shared use of expensive technology resources. Technologies such as server virtualization and partitioned multi-user software applications and databases make such sharing possible. These technologies do not come without risk, however. Configuration changes made by or for one customer can expose the systems and data utilized by other customers to breaches. Hacking

6 *Id.*

7 *Id.*

8 *Id.*

9 *Id.*

10 HIPAA Administrative Simplification Statute and Rules, U.S. Department of Health and Human Services, available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html>.

11 State Security Breach Notification Laws, National Conference of State Legislatures, available at <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>.

12 NIST Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, National Institute of Standards and Technology, U.S. Department of Commerce (December 2011), 17, available at <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>.



attempts that target virtual environment software (e.g., hypervisors) can compromise the security of both isolated and shared systems.<sup>13</sup> Strong security mechanisms must be implemented and regularly maintained to protect virtual, shared computing environments.

### Physical Security

For many healthcare organizations, cloud computing data centers can offer a level of physical security that they cannot begin to afford. Often built to withstand hurricanes, tornadoes, and other natural disasters, and equipped with state-of-the-art physical access authorization and control systems bolstered by on-premise security staff and video surveillance systems, these data centers can provide a robust environment to protect from physical damage and intrusion. Sound controls should be in place to provide assurance that all physical access is carefully controlled and monitored. Physical access should be provided only to those who have been authorized by the organization and those who work for the CSP, with timely communication and frequent reviews performed to remove those whose access is no longer permitted (e.g., a terminated employee). When necessary, additional controls should be utilized to further segregate hardware and storage media belonging to or utilized for multiple customers from each other, and protect against the compromise of shared communications circuits.

### Logical Security

Hosting application software and data in the cloud requires electronic access by both healthcare organization staff (i.e., as users and possibly as systems administrators) and CSP staff (i.e., as systems administrators). It may also involve access by third-party support staff, patients, consultants, auditors, regulators, and other individuals. Additionally, the use of the Internet, wireless access points, and mobile devices such as laptops, tablets and smartphones, increases the risks for unauthorized access.

Strong user authentication and access controls should be deployed, including the use of unique user IDs and strong passwords for normal user access, and separate user IDs and lengthier passwords or passphrases for those with privileged user and system administrator access.<sup>14</sup> Strong passwords are at least eight characters in length and contain a combination of upper case and lower case letters, one number and at least one special character.<sup>15</sup> Strong passwords should not contain dictionary words or

personal information<sup>16</sup> that can be readily obtained from other sources, such as public records and social networking sites.<sup>17</sup>

For more robust security, consideration should be given to using multifactor authentication, something that is quite common in financial and government industries, but is becoming more common in healthcare.<sup>18</sup> Multifactor authentication utilizes two or more types of credentials for authentication: “something you know” (password, transaction history, preselected graphic), “something you have” (token, proximity card, cryptographic key, IP-address), and “something you are” (fingerprint, retinal image, voice print).<sup>19</sup>

In addition to the use of unique user IDs, strong passwords, and multifactor authentication, additional access controls should be considered, such as: password history (password cannot be the same as any of a specified number of previous passwords); mandatory password expiration interval (password must be changed after a specified timeframe); password remembering ban (not allowing user IDs and passwords to be automatically populated); mobile access restrictions (not allowing mobile access or only allowing access from authorized, secure mobile devices); automatic inactivity logoff; lockout after a specified number of failed attempts (be careful with this one, it can make systems vulnerable to denial of service attacks and increase technical support demands); multiple session prohibition (users can only have one active logon session); DNS restriction (only allow access from specific network domains); and country restrictions (prohibit access from specific countries).

It should be noted that due to the shared nature of multi-tenant computer systems and built-in or self-imposed technical limitations, customized variations in minimum password requirements, multifactor authentication, and other authentication restrictions may not be available. In fact, some CSPs with the goal of operational simplicity and support cost control do not enforce minimum password length, complexity and other requirements for customer users, relying instead on their customers to train and monitor users on the creation and use of authentication credentials. Limitations like these can certainly pose a problem for healthcare organizations needing more stringent controls.

Regardless of the methodology and configuration used for user and administrator access authentication, additional controls should be in place to ensure that all access is properly requested and approved, that access rights are appropriate to each user’s job responsibilities (i.e., minimum necessary access),

13 NIST Special Publication 800-144, 11, 28; Cloud Computing: Virtual Cloud Security Concerns, Microsoft TechNet Magazine (December 2011), available at <http://technet.microsoft.com/en-us/magazine/hh641415.aspx>.

14 *CyberSecurity, 10 Best Practices for a Small Health Care Environment*, The Office of the National Coordinator for Health Information Technology (accessed June 26, 2013), available at <http://www.healthit.gov/providers-professionals/cybersecurity>.

15 *Id.*

16 *Id.*

17 *Feds require multifactor authentication for Health IT*, SecureIDNews (February 4, 2013), available at <http://secureidnews.com/news-item/feds-require-multifactor-authentication-for-health-it/#>.

18 NIST Special Publication 800-62-1, *Electronic Authentication Guideline*, National Institute of Standards and Technology, U.S. Department of Commerce (December 2011), 20, available at <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>.

19 NIST Special Publication 800-144, 24.



that access rights are periodically reviewed and vetted, and that appropriate separation of duties is enforced. With Internet and mobile access being the norm for cloud computing services, it is very important that access is removed in a timely manner for terminated users and for those whose job responsibilities change and physical access to an organization's computers is no longer required. Access logs and other management reports should be generated and reviewed, especially with respect to access to information about VIPs and those receiving medical treatment that may be of confidential or sensitive nature. The activities of users with privileged and administrator access should also be logged and reviewed for appropriateness. This is particularly important in virtual environments where server, software, database, network, and security administrator roles can overlap or be shared by customer, CSP and third-party staff, blurring accountability and inhibiting visibility into the tasks performed. Of course, these controls should not only be applied to CSP systems, but extended also to customer systems that are connected to or used to access CSP systems.<sup>20</sup>

### Encryption

Encryption of data at rest and in motion is a prudent safeguard designed to protect data from unauthorized access. It can also be an effective safe harbor resulting “in covered entities and business associates not being required to provide the notification otherwise required by section 13402 [of the HITECH ACT] in the event of a breach.”<sup>21</sup> Encryption scrambles data in such a way that, without the corresponding encryption key, the data is rendered unusable, unreadable, and indecipherable. Encryption can be implemented throughout the information technology continuum. Although it provides tangible benefits, it can certainly increase complexity and cost. The availability and type of encryption will vary according to technological and financial capabilities of both the CSP and the customer. Encryption should be considered in response to an in-depth security risk analysis, with careful consideration given to high risk areas such as Internet access, mobile devices, and the communications connections between the organization and the CSP. It is important to note that encryption does have limitations, and must be combined with other security controls to provide a complete security management program.

### Intrusion Detection, Prevention and Response

The data breach notifications required by the HITECH ACT (modified by the Omnibus Final Rule) and state data breach notification laws require ongoing vigilance and timely response

to actual and suspected breaches. This is especially important for organizations whose in-house systems and networks are closely or even directly integrated with cloud computing systems. The enormity and complexity of many cloud computing services environments can obscure the recognition and lengthen the analysis of breach incidents.<sup>22</sup> It is imperative that CSPs implement appropriate network and system defenses (e.g., firewalls, antivirus software, anomaly detection, and intrusion detection and prevention systems) which are designed to provide timely detection, threat defense, and incident notification. These coupled with thoughtfully designed and well-rehearsed incident response procedures will allow the CSP to respond quickly and effectively to limit the impact of security threats and breaches, and provide timely notification to the healthcare organization.

### Change Management

Hardware and software systems require frequent maintenance to facilitate high performance. They also require functional and security changes to ensure that they meet the needs of the users and are protected from emerging threats. With cloud computing services, changes may be applied to single customer systems or applied to systems used simultaneously by multiple CSP customers. Changes should be applied in an organized and well-tested manner so that they minimize disruption and preserve the integrity of the systems, data, and security defenses. This becomes more complicated in an environment in which changes are performed by individuals with varying skill levels and by individuals working for the CSP, the healthcare organization, and, in some cases, third-party subcontractors. The lack of a clear understanding regarding the responsibility, timing, documentation, testing, and other aspects of changes can have unintended and often detrimental effects on the confidentiality, integrity, and availability of systems and data.

### Data Deletion and Disposal

At some point in time, data will be deleted. Deletion will occur during normal use and in the maintenance of application and storage systems. Deletion will also occur when software and data become corrupted, when hardware fails, when systems are retired from service, and when the contractual relationship with the CSP ends. Not only can customer data be deleted, but activity and compliance logs required for security monitoring and compliance may be destroyed as well. Deletion, whether intended or accidental, has serious implications for ongoing operations, disaster recovery, regulatory compliance, and electronic discovery. The responsibility of both users and the CSP related

20 *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009*, Department of Health and Human Services (April 27, 2009), available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>.

21 NIST Special Publication 800-144, 33.

22 *Cloud Computing for Health Care Organizations*, Foley & Lardner LLP (October 2012), 16, available at <http://www.foley.com/cloud-computing-for-health-care-organizations-11-26-2012/>.

to data management and deletion must be well documented and monitored. Similarly, there should be explicit obligations to return data in an agreed-upon format when the contract ends and to ensure that all customer data stored on CSP systems is securely and irretrievably destroyed.<sup>23</sup>

### Data Use Rights

CSPs use analytical data concerning systems and network response times, utilization, intrusion detection, and other operational metrics to enable them to effectively manage, defend, and bill for their services. They may also want to utilize customer data, individually or aggregated with data from other customers, for their own commercial purposes. The permissible use of customer data must be clearly defined and understood to ensure that such use is not only acceptable to the healthcare organization, but is also restricted to uses allowed under HIPAA and other privacy and security regulations.<sup>24</sup>

### Staffing

One of the most tangible benefits of using cloud computing services is access to skilled and experienced information technology staff. The size of large-scale CSPs typically provides an opportunity for staff to specialize, especially in the areas of privacy and security.<sup>25</sup> Such specialization can provide a higher level of performance than may be available to many healthcare organizations, especially small to mid-sized entities. Workforce screening, training, and monitoring are as critical employment and contracting practices for CSPs as they are for any organization, but especially for those individuals who are entrusted with managing and protecting critical systems and confidential data. Healthcare organizations should request information regarding CSP employment practices, the education, training and certifications achieved by CSP employees, and the processes used to monitor and manage employee performance.

### Oversight and Assurance

One of the common concerns associated with third-party provided services, including cloud computing services, is limited visibility into the third-party provider's internal practices and controls. In the case of CSPs, some degree of obscurity is required in order to protect the security of CSP systems. Service agreements should include access to performance and security

reports, as well as the right to inspect and audit controls or obtain an independent third-party report regarding controls that are not accessible or assessable. Some CSPs will provide information regarding their security controls and regulatory compliance programs. Others will allow customer auditors to perform an assessment of their internal controls. Large CSPs typically engage qualified third-parties such as CPAs and assessors authorized by standards organizations to perform assessments that are shared with their customers. Some CSPs implement formal programs to achieve specific security certifications and assurances relevant to the services they provide or the types of organizations they serve. Here are examples of reports, certifications, and assurances that healthcare organizations may find useful in their efforts to gain visibility into a CSP's privacy and security controls.

**Service Organization Control Reports** – Service Organization Control (SOC) reports provide information about the internal controls related to an outsourced service that users (such as healthcare organizations) can use to assess and address the risks associated with an outsourced service.<sup>26</sup> There are three types of SOC reports: SOC 1<sup>SM</sup>, SOC 2<sup>SM</sup>, and SOC 3<sup>SM</sup>. SOC 1 reports are useful to users and user auditors in evaluating the effect of the controls at the service organization on the user entities' financial statements. SOC 2 reports provide information about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. SOC 3 reports are designed to meet the needs of users who need assurance about the controls at a service organization that affect the security, availability, and processing integrity, confidentiality, or privacy, but do not need or have the knowledge necessary to make effective use of a SOC 2 report. The AICPA's website and publications provide details regarding the scope, use, and distribution of these reports.<sup>27</sup>

**ISO/IEC 27001:2005** – This is a standards specification for implementing, managing, and maintaining an information security management system in all types of organizations. It provides detailed requirements for implementing security controls.<sup>28</sup> Certification of compliance with the standard is available through authorized third-party assessment organizations.<sup>29</sup>

23 Foley & Lardner LLP, 15.

24 NIST Special Publication 800-144, 9.

25 *Service Organization Control Reports*, American Institute of CPAs, (accessed June 26, 2013), available at <http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx>.

26 *Id.*

27 ISO/IEC 27001:2005, International Organization for Standardization (accessed June 26, 2013), available at [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103).

28 *The ISO27001 Certification Process* <http://www.27000.org/ismsprocess.htm>.

29 NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, U.S. Department of Commerce (August 2009 with updates as of May 1, 2010), available at [http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final\\_updated-errata\\_05-01-2010.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf).

### ***Federal Risk and Authorization Management Program***

**(FedRAMP)** – A cloud service provider that wants to provide services to one or more federal agencies must implement the controls specified in NIST Special Publication 800-53 and have a third party assessment organization perform an independent assessment of the implementation of these controls. The FedRAMP Joint Authorization Board (JAB) reviews the security assessment package and may grant a provisional authorization for cloud services that can be used as an initial approval that federal agencies can leverage in granting security authorizations and an accompanying authority to operate for use.<sup>30,31</sup>

### ***Payment Card Industry (PCI) Data Security Standard (DSS)***

PCI DSS provides a framework for developing a payment card data security process which includes prevention, detection, and response to security incidents.<sup>32</sup> It comprises a minimum set of requirements for protecting cardholder data.<sup>33</sup> It is applicable to CSPs that store, process or transmit cardholder data. Such CSPs can engage Qualified Security Assessor companies to validate an entity's adherence to the PCI DSS.<sup>34</sup> CSPs can also engage Approved Scanning Vendors to validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments.<sup>35</sup>

### ***Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)***

– STAR is a public registry that documents the security controls provided by various cloud computing service offerings. Its purpose is to help users assess the security of cloud services providers they use or are considering using.<sup>36</sup> CSPs post self-assessments performed using the CSA's Consensus Assessments Initiative Questionnaire, which is based on the controls specified in CSA's Cloud Controls Matrix.<sup>37</sup>

In addition to these reports, certifications, and self-assessments, CSPs may also provide specific information concerning the programs they have implemented to comply with HIPAA and other federal and state privacy and security regulations.

### **Understand and Be Vigilant**

Like clouds that come and go with changing weather, cloud computing will continue to change and evolve, often in dynamic and paradigm-changing ways. Consideration of the privacy and security risk areas identified in this article is just the beginning of understanding and vigilance, much like reading a weather report before venturing outside. Healthcare organizations that use cloud computing services must implement thorough evaluation, monitoring, and risk assessment programs to ensure the privacy and security of PHI and other confidential information in order to keep the “clouds” from raining on their parade. ♦

30 *FedRAMP Security Assessment*, U.S. General Services Administration (accessed June 26, 2013), available at <http://www.gsa.gov/portal/category/102999>.

31 *PCI SSC Data Security Standards Overview*, PCI Security Standards Council (accessed June 26, 2013), available at [https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php).

32 *Payment Card Industry Data Security Standard – Requirements and Security Assessment Procedures, Version 2*, PCI Security Standards Council (October 2010), 5, available at [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf).

33 *Qualified Security Assessor Companies*, PCI Security Standards Council (accessed June 26, 2013), available at [https://www.pcisecuritystandards.org/approved\\_companies\\_providers/qualified\\_security\\_assessors.php](https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php).

34 *Approved Scanning Vendors*, PCI Security Standards Council (accessed June 26, 2013), available at [https://www.pcisecuritystandards.org/approved\\_companies\\_providers/approved\\_scanning\\_vendors.php](https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php).

35 *CSA Security, Trust & Assurance Registry*, Cloud Security Alliance (accessed June 26, 2013), available at <https://cloudsecurityalliance.org/star/faq/>.

36 *Id.*

# Your Essential Resource for Fraud and Compliance Issues



**T**he American Health Lawyers Association (AHLA) is the nation's largest, nonpartisan, 501(c)(3) educational organization devoted to legal issues in the healthcare field. Our network of more than 12,500 members represents the best professionals in the healthcare legal and regulatory field. AHLA members receive news about the latest developments in enforcement activities, analyses from noted experts, and have access to insightful and practical resources.

AHLA gives you the opportunity to network with leading compliance and privacy officers, attorneys, finance officers, healthcare consultants, regulatory professionals, providers, CEOs, public health officials, and others from across the country, recognized as movers and shakers in the health care community.

Join AHLA as a new member and also receive free enrollment in the Fraud and Abuse Practice Group, which provides benefits such as:

- » Email alerts on enforcement activity such as settlements, judicial opinions, and indictments;
- » Newsletters, and member briefings providing detailed information and analysis of relevant topics;
- » Detailed summaries of OIG and CMS Advisory Opinion as they are issued;
- » Substantial savings on webinar bootcamp series, individual webinars, and luncheons as well as free roundtables on fraud and abuse topics; and
- » Online Practice Corner, where portions of the information above are kept for ease of viewing anytime.

**Join AHLA today!**

[www.healthlawyers.org/members](http://www.healthlawyers.org/members) (202) 833-1100, prompt #2

**YOUR MISSION | OUR SOLUTIONS**

Strategy | Operations | Technology

## Research Enterprise Management

### Our Services Include:

- Research Administration Transformation
- Compliance Investigations & Risk Management
- Facilities & Administration (F&A) Cost Recovery Services
- Research Strategy Facilitation & Financial Planning
- Interim Management & Staffing
- Research Software Solutions



## BRINGING EXCELLENCE ACROSS THE INSTITUTION.

**The best results are derived from team efforts.** Huron's Research Enterprise Management solutions improve every aspect of research administration performance. Our solutions and deep expertise enable clients to more effectively manage the business of research, improve financial management and cost reimbursement, improve service to faculty, and mitigate compliance risks. To see how our solutions can impact your mission, visit [www.huronconsultinggroup.com/research](http://www.huronconsultinggroup.com/research).

**1-866-229-8700**  
**[huronconsultinggroup.com/research](http://huronconsultinggroup.com/research)**

© 2013 Huron Consulting Group Inc. All Rights Reserved.

# Huron



# Structuring An Effective And Efficient Research Compliance Program

*Anne Sullivan, Senior Director, Huron Consulting Group*

*asullivan@huronconsultinggroup.com*

*Leah Guidry, Managing Director, Huron Consulting Group*

*lguidry@huronconsultinggroup.com*

*Allecia Harley, Director, Huron Consulting Group*

*aharley@huronconsultinggroup.com*



## Introduction

Research is the production backbone of innovative healthcare; helping many institutions discover and develop new drugs, devices, technologies, and approaches to care that enable patient recruitment, building a reputation for high quality care, and for some, to stay afloat financially. Research runs the gamut from laboratory, animal, and human subjects to broad data-based inquiries about population health and approaches to care delivery. While the benefits of innovative research are many, those benefits do not come without regulatory and financial compliance risks. This article outlines practical steps to build an approach and an infrastructure in the highly specialized area of research compliance and to minimize the impact of the risks associated with research.

## Research Compliance Climate

The current research climate demands strengthened and specialized compliance programs that will monitor and mitigate a wide range of internal and external risks. The last decade has seen an increase in the development of research compliance programs, offices, and units within institutions; these offices are now facing unprecedented pressure to adapt to a changing research climate.

Research institutions are facing an increasing number of regulatory changes. In just the past few years, the industry has seen revised conflict of interest regulations, proposed changes to OMB Circulars, clinical trial disclosure requirements, and modifications to HIPAA laws, just to name a few. As a result, research compliance units are confronting mounting compliance expectations in the era of transparency and accountability. Funding

decreases and sequestration of funds also create pressures that, when coupled with the increased regulatory changes, heighten the challenges facing these programs.

The increased complexity of both financial and regulatory management of research means that compliance offices are continually challenged to increase their capacity for technical knowledge and regulatory acumen. The implementation of programs to assess the institution's ability to comply as well as personnel to monitor that compliance is increasingly challenging. Research compliance programs must be able to monitor and react to increased regulatory complexity with decreasing resources and the internal need to build and manage programs; essentially doing more with less.

In addition, a growing number of fiscal reporting requirements and a greater focus on accountability and transparency make it necessary for research compliance programs to monitor an increasing volume of fiscal activities. The federal focus on accountability and transparency began as a hallmark of the first Obama administration. The President called for federal agencies to intensify efforts to improve reporting compliance and to enforce sanctions for noncompliance, such as terminations of research awards, suspension or debarment, or implementing punitive actions under the American Recovery and Reinvestment Act of 2009.<sup>1</sup> Additionally, federal auditors and Inspectors General continue to focus on compliance with cost principles that govern effort reporting, fraudulent billing, direct charging of administrative costs on research projects, and, most recently, a false grant renewal application.<sup>2</sup> The U.S. Department of Health and Human Services (HHS) Office of the Inspector General (OIG) Work Plan provides further evidence to research compliance professionals

<sup>1</sup> 75 Fed. Reg. 18045, April 8, 2010 The American Recovery and Reinvestment Act (ARRA) of 2009 allocated an unprecedented \$787 billion to help stimulate the nation's economy, including \$21.5 billion in federal research and development funding. ARRA included extraordinary regulatory and other compliance requirements and provided separate appropriations for agency inspectors general and the Government Accountability Office to monitor stimulus spending.

<sup>2</sup> Workmaster, Jason. *Government Contracts Advisor*. September 12, 2012. <http://www.governmentcontractsadvisor.com/2012/09/12/second-circuit-upholds-fca-liability-assessment-against-grantee-for-entire-value-of-grant-renewal/> (accessed June 6, 2013).

## Financial Compliance Issues

- Account overdrafts
- Administrative costs
- Award close outs
- Billing compliance
- Cost sharing
- Cost transfers
- Direct charging practices
- Effort reporting
- Equipment claims
- Extra service compensation
- Program income
- Recharge centers
- Unallowable costs

## Non-Financial Compliance Issues

- Animal subject protections
- Conflicts of interest
- Environmental health and safety
- Export controls
- HIPAA privacy and security
- Human subject protections
- Invention disclosures and reporting
- Responsible conduct of research
- Scientific overlap
- Scientific misconduct
- Sub awardee monitoring
- GxP compliance and monitoring
- ClinicalTrials.gov reporting

of the government's focus on fiscal reporting and the need to monitor the same.<sup>3</sup> The current Work Plan gives clues to the federal government's priority focus areas, such as extra service compensation payments for faculty on research funds, inappropriate salary draws from multiple institutions, equipment claims by research grantees, and cost sharing claimed by research institutions. Furthermore, there is a real and perceived threat of potential whistleblower or qui tam settlements under the civil False Claims Act due to a high number of cases focused on federal research in recent years.<sup>4</sup> In addition, the Internal Revenue Service (IRS) recently audited approximately thirty universities and found that they underpaid their unrelated business income taxes (UBIT) by nearly \$90 million.<sup>5</sup> These examples demonstrate the degree of financial oversight by the federal government resulting in increased pressure for institutions to manage and monitor financial compliance in a widening range of subject matters.

Non-financial regulatory trends have seen similar increases in focus, desire for transparency, and monitoring requirements, all of which place pressure on research compliance programs. A relatively recent focus is on the responsible conduct of research (RCR) regulations under the governance of the NSF America COMPETES Reauthorization Act of 2010.<sup>6</sup> The Act requires that each institution submitting applications for NSF research funds provide training and oversight in the responsible and ethical

conduct of research to undergraduate students, graduate students, and postdoctoral researchers participating in the proposed research project.<sup>7</sup> In fact, it was recently announced that the National Science Foundation OIG will conduct RCR assessments of universities' compliance with the new RCR regulations.<sup>8</sup> Additional areas of non-financial regulatory and compliance changes include the FDA's establishment of a publically accessible clinical trial registry database, which serves as an oversight mechanism to ensure proper reporting and transparency of clinical trials results.<sup>9</sup> Additionally, HIPAA now requires HHS to perform audits to ensure that covered entities are complying with its regulations and breach notification standards. In short, these HIPAA audits aim to identify best practices and methods for compliance as well as focus institutional attention on compliance risks.<sup>10</sup> Finally, changes to HHS' amended conflict of interest (COI) regulations, which took effect in August 2012, mandate training for investigators and reporting of royalty income and reimbursed sponsored travel.<sup>11</sup>

This widespread, yet non-exhaustive, list of diverging financial and non-financial regulatory compliance issues creates a complex charge for the research compliance program at an institution: (see [chart above](#))

3 Office of the Inspector General Work Plan, Fiscal Year 2013.

4 Ferreira, William F., Anne M. Sullivan, and Michael J. Vernick. "The False Claims Act and Fraud Allegations in Sponsored Research." *NACUA CLE Workshop*. Washington, DC: NACUA, 2010. 1, 7-10, 13-30.

5 Kelderman, Eric. *34 Colleges Underpaid Federal Taxes by \$90-Million, IRS Says*. April 26, 2013. [http://chronicle.com/article/34-Colleges-Underpaid-Federal/138833/?cid=at&utm\\_source=at&utm\\_medium=en](http://chronicle.com/article/34-Colleges-Underpaid-Federal/138833/?cid=at&utm_source=at&utm_medium=en) (accessed June 6, 2013).

6 "America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education and Science (COMPETES) Act." *42 U.S.C. 18620-1*. National Science Foundation, 2010.

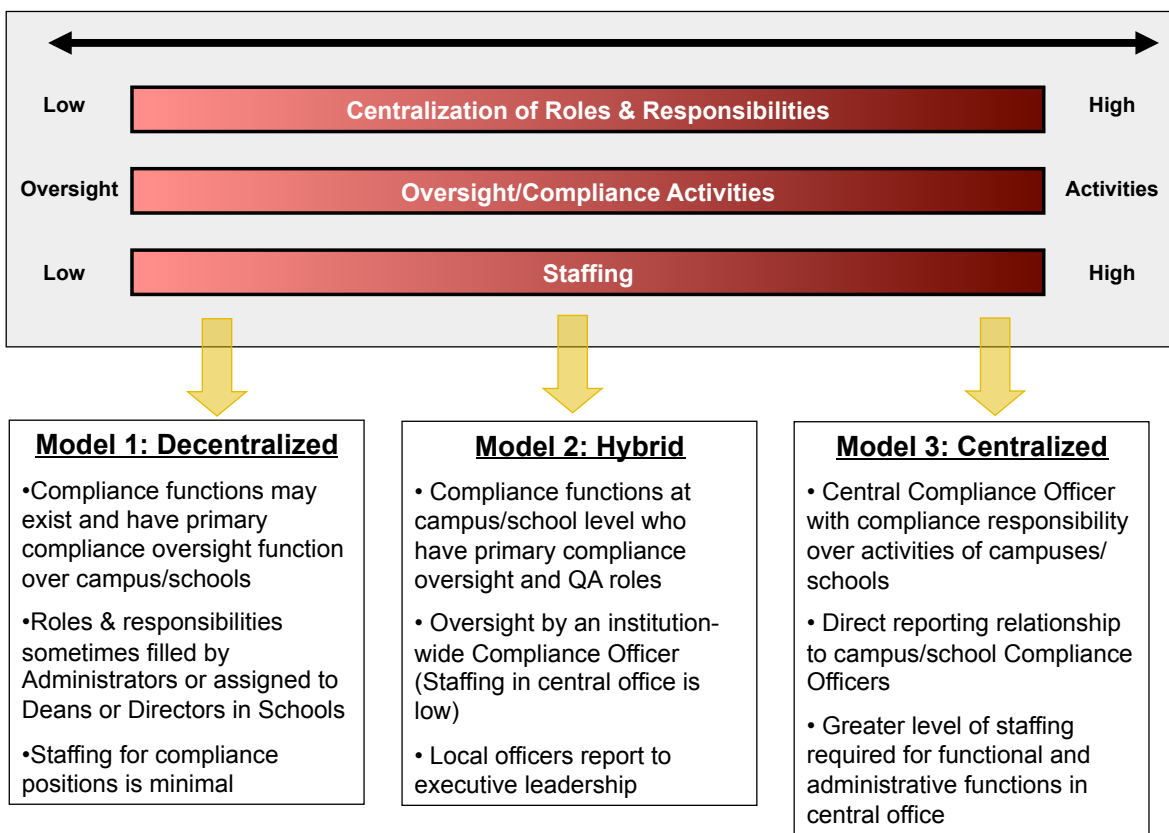
7 Foundation, National Science. n.d. [http://www.nsf.gov/about/congress/110/highlights/cu07\\_0809.jsp](http://www.nsf.gov/about/congress/110/highlights/cu07_0809.jsp).

8 Lerner, Allison. "We're In This Together!" *NCURA Magazine*, March/April 2013: 15.

9 Gaffney, Alexander. *Regulatory Focus*. September 25, 2012. <http://www.raps.org/focus-online/news/news-article-view/article/2299/fda-given-new-authority-to-oversee-clinical-trials-data-reporting.aspx> (accessed June 6, 2013).

10 Sanches, Linda MPH. "HIPAA Privacy, Security and Breach: Program Overview & Initial Analysis." *HCCA 2013 Compliance Institute*. 2013. 17.

11 42 C.F.R. Part 50, Subpart F.



Source: Huron Consulting Group

The research regulatory climate is changing rapidly and the research compliance program must monitor and oversee emerging issues in an efficient manner while taking care not to assume operational responsibility for managing them.

### Research Compliance Programs – Size & Structure, Reporting & Governance, and Components and Personnel

Institutions looking to create an effective and efficient research compliance program must consider a variety of issues including program size and structure, reporting lines, and areas of focus. Influencing each of the decisions about these issues are the institutional type, institutional culture, the amount and complexity of the research portfolio, as well as the institutional risk tolerance.

Decisional influences are as important as the decision-making itself because awareness of the context of the decisions enables full consideration and diligence. Academic medical centers are vastly different from community hospitals and, as such, their research compliance programs need to recognize these differences and develop effective structures to meet the needs of their institution. Similarly, institutions that exert considerable control or top-down management style will have very different needs from organizations that function comfortably with a matrix management approach and looser models of decision-making. Finally, tolerance for risk influences the number and strength of internal controls needed in the compliance program.

### Size and Structure

Influencing the size and structure of the research compliance program are the needs of the program, the type of program implemented, and the diversity and volume of research portfolio itself. There are several questions and considerations when establishing the infrastructure of a research compliance program, including:

- » What is the scope of the research portfolio and what will be the scope of the research compliance program? For research programs with a narrow scope, what are the rules of engagement for referrals to other related oversight areas (e.g., faculty misconduct) and how are these issues monitored in those other oversight areas to ensure resolution?
- » How do you establish either segregation or integration of health care compliance from research compliance?
- » Should a dedicated research compliance role/position be created?
- » Which compliance content areas should have their own compliance infrastructure (i.e. HIPAA/FERPA, faculty issues, etc.)?

The essential theme of these questions is how focused and integrated research compliance should be with respect to other units within the organizational structure. Exploring each of these

	Decentralized	Centralized	Hybrid
STRENGTHS	<ul style="list-style-type: none"> <li>• Traditional structure, well-understood in higher education</li> <li>• Oversight by the areas that are closely aligned with primary functions</li> <li>• Can ensure appropriate controls and compliance as its more closely connected w/ operations function</li> </ul>	<ul style="list-style-type: none"> <li>• Enables increased communication</li> <li>• Less possibility for duplication of effort</li> <li>• Strong leadership presence that may promote increased service to the institution and balanced prioritization of investments in resources to manage compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Enables increased communication</li> <li>• Less possibility for duplication of effort</li> <li>• Strong operations leadership that may enhance efficiency and coordination with other functions</li> </ul>
WEAKNESSES	<ul style="list-style-type: none"> <li>• Potential for gaps in communication</li> <li>• Potential for duplication in efforts</li> <li>• Potential for confusion in role for operations and balanced oversight</li> </ul>	<ul style="list-style-type: none"> <li>• Oversight by an individual that has numerous priorities that could be in conflict with optimizing compliance and administration</li> <li>• Potential risk for compliance issues (in practice) - lack of local oversight</li> </ul>	<ul style="list-style-type: none"> <li>• Potential for less of a focus on services and more of a focus on compliance</li> <li>• Potential risk for jurisdiction and management conflicts</li> </ul>

Source: Huron Consulting Group

questions in detail to determine the appropriate structures helps to customize the program. Yet ultimately, compliance effectiveness depends on the culture of an institution as well as how the reporting relationships strengthen and align with the institution's mission and vision.

### Sample Models for Compliance

The graphic above illustrates three sample models for compliance frequently established for research compliance programs; decentralized, centralized, and a hybrid of the two. The graphic assumes that there is a central compliance office or unit established at an institution, with each model depicting the degree of centralization of roles and responsibilities, oversight and staffing of the central office; essentially the degree of control or oversight that the central compliance office or unit has on the research enterprise.

Structural models for research compliance programs fall along a continuum from highly decentralized to highly centralized. In a decentralized model, the compliance personnel and functions are closely aligned with the operational units themselves and the compliance personnel in these models may have other responsibilities. The centralized models have centrally reporting personnel that tend to have a singular focus on compliance.

The benefit of decentralization is that the compliance functions are more likely embedded into the operational aspects of research. Compliance personnel work alongside research personnel and, as a result, can identify problems more readily and may be able to address these problems organically as part of their working relationship. One major weakness in a decentralized

model is the degree to which this close relationship causes the compliance function to lose its independent character – a function that is so important to the integrity of the compliance effort.

Conversely, the benefit of a centralized model is that it allows for the maintenance of this independence – both perceived and actual. One downfall of the centralized model is that the central compliance professional can be viewed as an outsider, which potentially jeopardizes the transparency necessary to identify and address compliance issues in a timely manner. Highly siloed organizations with centralized compliance functions are particularly vulnerable to this downfall.

One suggested structural approach is to embed the research compliance personnel into the operational units with solid line reporting to centralized compliance leadership and dotted line reporting to the operational leadership. Coupled with this is the need for a centralized auditing and monitoring function to review the compliance implementation within those units. This structure addresses the desire to have a close connection between the compliance personnel and the operational personnel as well as the need to maintain the independence of the compliance function through the centralized monitoring and auditing function.

The chart above outlines a framework for comparing the various models according to their strengths and weaknesses:

Finally, in making choices about the size and structure of the research compliance program, research institutions should evaluate the size and scope of their research portfolio, consider their existing culture, and choose one of the models described above that best fits the strategic direction of their enterprise.



## Governance and Reporting Relationships

Along with defining a program structure, it is important to determine the appropriate governance and reporting structure and the level of day-to-day program oversight. Corporate Integrity Agreements signal the government's bias for having the compliance officer report to senior levels of institutional leadership and to have direct lines of access to the institutional governing authority. More important than the reporting relationship to the effectiveness of the program, however, is whether the Research Compliance Officer (or other functional title) is an individual who occupies a key position in the organizational structure and who has the authority to enact change.

Strong and effective compliance offices necessitate senior-level leadership support for the change initiatives necessary for achieving compliance in a highly regulated and changing climate. Compliance offices must ensure coordination with various central leaders and local, unit leaders. A compliance leader cannot be successful without organizational support for the compliance program and structure, nor can they be successful without strong relationships with senior leaders. Focused support from the organization's senior officials and departmental leadership can serve as pillars for the compliance program. Equally important, the compliance officer must have a communications channel and access to those senior officials.

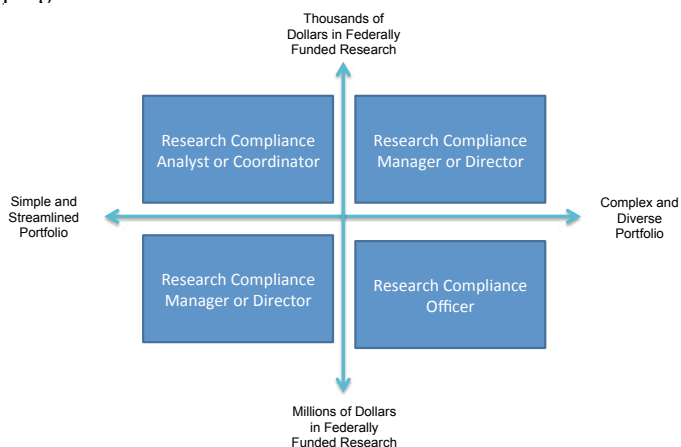
Establishing reporting lines to give the research compliance leadership oversight and responsibility for the entire research compliance program is important. Oversight and responsibility do not mean that the compliance leader has operational responsibilities for carrying out compliance for each subject matter, however. Senior administration within the organization will have specific operational responsibilities for subject matters, which the compliance program will need to review and ensure are functioning properly. This is true at the department level as well as within central operational units. For instance, the Chair of Hematology may have operational responsibility for both the delivery of clinical care as well as research occurring in this area; and the Clinical Trials Office, Pre and Post Award Units, are responsible for service delivery in a compliant manner. Finally, there are specific areas of operation in research that have significant compliance components, such as the Institutional Review Board (IRB) and the Institutional Animal Care and Use Committee (IACUC).

Once these oversight or operational responsibilities are defined, an institution must ensure that research compliance offices have reporting lines that allow for strong communication and optimization of information flow within and between compliance units, administration and operating units. Mechanisms for reporting compliance between units, up to leadership, and down to administrators and researchers should be well integrated into daily practice.

Despite varying structures or reporting lines, leadership needs to demonstrate a commitment to invest in improvement and in change initiatives necessary to achieve compliance across

the entire program. Regardless of the governance approach, the research compliance program should have a designated leader who, at a minimum, coordinates all aspects of the program, its personnel, and the varying issues that arise in a busy research enterprise. Larger institutions will appoint a chief officer or director in charge of research compliance, while smaller institutions may include the expertise in their broader team.

The graphic below illustrates a methodology for determining the level of leadership and/or support an institution needs for its program:



Source: Huron Consulting Group

Regardless of the specific title of the position, the basic skills needed for research compliance are the same:

- » Ability to review and interpret federal regulations and guidance in order to spot issues, and clearly communicate the regulations and guidance
- » Effective relationship development skills and emotional intelligence to influence cultural and behavioral changes in the organization
- » Understanding of clinical research principles, strategy, and execution
- » Familiarity with the breadth of bench, animal, and clinical research compliance concerns
- » Integrity and transparency in action, communication, and decision-making
- » Demonstrated ability to implement the kind of tasks outlined in the eight components of a research compliance program

In addition to the support afforded by the leadership of the institution and its various departments, many institutions see the need to create a committee that is specific to research. Research compliance is highly nuanced and involves complex and ever changing governing regulations. This environment makes a

specialized committee charged with providing guidance a valuable resource. The committee should include representatives from the research community with expertise in the areas of focus to help guide the response to issues that arise. The committee should be a part of the governance structure and could have permanent as well as ad hoc members when support is needed in specific content areas.

## **Program Components and Personnel**

### ***Elements of a Research Compliance Program***

Hospitals and health systems have well developed healthcare compliance programs based on federal guidance.<sup>12</sup> This guidance for hospitals is similar in many ways to the draft guidance for researchers with federal grant awards.<sup>13</sup> Aside from the differences in the subject matter, the greatest distinction between the OIG's approach to a general healthcare compliance program and a research compliance program is the addition of an eighth element. The eight elements as outlined in the guidance are below:

1. Implementing written policies and procedures,
2. Designating a compliance officer and compliance committee,
3. Conducting effective training and education,
4. Developing effective lines of communication,
5. Conducting internal monitoring and auditing,
6. Enforcing standards through well-publicized disciplinary guidelines,
7. Responding promptly to detected problems and undertaking corrective action, and
8. Defining roles and responsibilities and assigning oversight responsibility.

Elements one through seven are well communicated and documented, but element number eight may not be familiar to all. One could argue that the eighth element is implied as a key component of the other seven. By calling it out separately, the OIG emphasizes this critical need within institutions that engage in research.

Research compliance programs should encompass these elements in much the same manner as the general healthcare compliance program, whether or not it follows the OIG's draft guidance by adding the eighth element.

### ***Trained and Knowledgeable Personnel***

Since research is highly specialized and varies from program to program, research compliance needs to be similarly specialized with personnel trained and skilled in the areas they oversee. Research compliance personnel need to possess general research knowledge, but also need to have expertise in their areas of focus (e.g., human subjects protections, post award fiscal oversight, clinical research billing).

## **Conclusion**

Research compliance is a complex area that benefits from the standard approach utilized in general healthcare compliance, with the addition of an eighth element. It does require a specific set of skills and the engagement of a crosscutting group of leaders. The approach, the structure/model, and the placement personnel should be customized to meet the needs of the institution but should also be evaluated regularly to ensure that decisions made are, in fact, serving the intended needs. Embarking on a research compliance endeavor requires detailed planning and strategic partnerships, but is well worth the effort to support the integrity of the research enterprise and safeguard the allocation of limited resources.

Using the points raised in this article will help in determining whether a research compliance program is needed, as well as the best structure and governance model for the program. Once these basic decisions are made, identifying the focus areas for the program and the compliance activities that will be handled elsewhere within the organization will further define the program. Ensuring adequate oversight of all areas is key. Finally, hiring personnel with the proper training and experience is essential to the successful management of research compliance in the organization. ♦

<sup>12</sup> Office of the Inspector General January 2005.

<sup>13</sup> Office of the Inspector General November 2005.

Compliance Requirement	Regulation	Summary	Related Risks
<b>Financial</b>			
<b>Account Overdrafts</b>	<ul style="list-style-type: none"> <li>• OMB Circ. A-21, C. 12. f.</li> </ul>	How to account for cost overruns on an award greater than the total budget.	<ul style="list-style-type: none"> <li>• Write-offs, deficits.</li> </ul>
<b>Administrative Costs</b>	<ul style="list-style-type: none"> <li>• OMB Circ. A-21, F. 6. b.</li> </ul>	Requires administrative and clerical expenses to be normally treated as F&A costs, not as direct costs except when the expenses are used to support a major project or activity. Items such as office supplies, postage, local telephone costs, and memberships shall normally be treated as F&A costs.	<ul style="list-style-type: none"> <li>• Charges for normal administrative support inappropriately charged as direct costs.</li> <li>• Pens, paper, clerical salary, postage, memberships, etc. are direct charged to grants in normal circumstances as opposed to unlike circumstances.</li> <li>• Large research centers/institutes do NOT distinguish unlike circumstances and charge administrative costs direct.</li> </ul>
<b>Award Closeouts</b>	<ul style="list-style-type: none"> <li>• OMB Circ. A-110, .70 - .73</li> </ul>	Process for reviewing at the end of an award.	<ul style="list-style-type: none"> <li>• Continuous charges, overspending the award.</li> </ul>
<b>Billing Compliance</b>	<ul style="list-style-type: none"> <li>• Medicare Claims Processing Manual, Chapter 32, Section 69</li> <li>• Medicare National Coverage Determinations Manual, Chapter 1, Part 4, Section 310.1 Routine Costs in Clinical Trials</li> <li>• USC §3729- Federal False Claims Act</li> <li>• State-specific False Claims Acts</li> </ul>	Proper identification of costs to ensure that all costs of a clinical trial are billed to the appropriate payer whether it is the sponsor, a third party payer or the patient/subject. The PI and provider/billing entity are responsible for compliance with all billing rules for billing Medicare, Medicaid, and third party insurers for services provided in the context of clinical research. The False Claims Act establishes criminal and civil penalties for knowingly submitting claims to the federal government, causing another to submit a false claim, or acting improperly to avoid paying monies due to the federal government. There may be similar regulations enacted at the individual state level.	<ul style="list-style-type: none"> <li>• Audits.</li> <li>• Corporate integrity / compliance agreements.</li> <li>• Fines.</li> <li>• Negative publicity.</li> <li>• False claim allegations.</li> <li>• Damage to the institution's and/or principal investigator's reputation.</li> </ul>
<b>Cost Sharing</b>	<ul style="list-style-type: none"> <li>• OMB Circ. A-110, .23</li> </ul>	Cost sharing is a commitment of university (or third party) resources or funding that supplements externally sponsored project funding. Additionally, mandatory cost sharing occurs when the sponsor has required cost sharing as a prerequisite to apply for and receive an award.	<ul style="list-style-type: none"> <li>• Mandatory cost sharing commitments are not met, unallowable/inappropriate charges used to meet cost sharing commitments.</li> <li>• Effort certification system does not verify cost sharing charges.</li> <li>• University does not record and maintain documentation for reporting the cost sharing to the funding agency.</li> </ul>
<b>Cost Transfers</b>	<ul style="list-style-type: none"> <li>• OMB Circ. A-110, .25</li> </ul>	A cost transfer is an after-the-fact reallocation of the cost associated with a transaction from one activity/account to another.	<ul style="list-style-type: none"> <li>• Insufficient documentation for cost transfers.</li> <li>• Significant number of late cost transfers (greater than 90-120 days after original charge).</li> <li>• Costs transferred from an account in overrun status to an account with large balance.</li> <li>• Significant number of cost transfers from departmental account to sponsored accounts.</li> </ul>

Compliance Requirement	Regulation	Summary	Related Risks
<b>Direct Charging Practices</b>	<ul style="list-style-type: none"> <li>OMB Circ. A-21: D. 1.-2.; F. 6. b. (1); Exhibit C</li> </ul>	Section D.1 of OMB Circular A-21 states: Costs incurred for the same purpose in like circumstances must be treated consistently as either direct or indirect costs. OMB Circular A-21 requires costs directly charged to a sponsored project to be: Allocable (provides direct benefit), Allowable (per university or sponsor policy or OMB Circular A-21), Reasonable and necessary, Consistently treated throughout the institution, and available within the budget for the award.	<ul style="list-style-type: none"> <li>Departmental charges distributed to multiple grants.</li> <li>Departmental or institute business manager allocated to multiple grants.</li> </ul>
<b>Effort Reporting</b>	<ul style="list-style-type: none"> <li>OMB Circ. A-21, J. 10. c. (1)-(3)</li> <li>OMB Circ. A-110 .17</li> <li>OMB Circ. A-122 Attach B - #7 m.</li> </ul>	Effort is the proportion of time spent on any activity and expressed as a percentage of the total professional activity for which an individual is employed by the institution. OMB Circular A-21, section J.10 requires an effort reporting system that: encompasses all employee activities, confirms effort expended after-the-fact, requires certification to be performed by an individual with knowledge of all of an employee's activities or suitable means of verification, and requires certification to be performed regularly.	<ul style="list-style-type: none"> <li>Institutional Base Salary (IBS) not clearly defined or consistently applied.</li> <li>Faculty members with teaching/admin/clinical responsibilities charging 100% of salary to sponsored projects.</li> <li>Effort dedicated to certain "K" awards less than 75 percent of total professional effort.</li> <li>Committed cost sharing not reported.</li> <li>Effort certified by person without first hand knowledge, and who did not use suitable means of verification.</li> <li>Incomplete effort distributions.</li> <li>Salary cap not considered.</li> <li>Lack of accurate and timely effort reporting (no certifications exist).</li> <li>Significant cost transfers.</li> <li>Committed effort is greater than 100 percent.</li> </ul>
<b>Equipment Claims</b>	<ul style="list-style-type: none"> <li>OMB Circ. A-110, .34</li> </ul>	The university retains ownership of or title to most capital equipment purchased with sponsored research funds. Equipment should not be sold, transferred, or otherwise disposed of without first notifying the university.	<ul style="list-style-type: none"> <li>Unallowable or unallocable equipment purchases.</li> <li>Equipment Disposal.</li> </ul>
<b>Extra Service Compensation</b>	<ul style="list-style-type: none"> <li>OMB Circ. A-21, J. 10. d (1)</li> </ul>	<p>Applies to employees who function as consultants for sponsored awards conducted under the direction of other university employees. Extra service compensation from external funds can be allowed for faculty when all of the following conditions are met:</p> <ul style="list-style-type: none"> <li>The request does not exceed the normal rate of pay based on the faculty member's institutional base salary</li> <li>Work is separate from or only remotely related to the employee's primary role assignment.</li> <li>Work is in addition to the full workload, which reflects the primary role assignment(s).</li> <li>The request is specifically proposed and included in the approved budget and/or agreement with the sponsoring agency or otherwise approved in writing by an authorized representative.</li> </ul>	<ul style="list-style-type: none"> <li>Inaccurate charging of salary and effort on sponsored awards.</li> </ul>

© Huron Consulting Group Inc. All Rights Reserved.



Compliance Requirement	Regulation	Summary	Related Risks
<b>Program Income</b>	<ul style="list-style-type: none"> <li>OMB Circ. A-110, .24</li> </ul>	<p>Program income is gross income earned by a grantee that was directly generated by the grant-supported activity or earned as a result of the award. Examples include: Fees for services performed, the use or rental of real or personal property acquired under the grant, the sale of commodities or items fabricated under an award, and license fees and royalties on patents and copyrights. NIH will specify how the income is to be used and whether the income needs to be reported to NIH and for what length of time. Unless otherwise specified in the terms and conditions of the award, NIH grantees are not accountable for program income accrued after the period of grant support.</p>	<ul style="list-style-type: none"> <li>Non-disclosure of potential program income on grant application.</li> </ul>
<b>Recharge Centers</b>	<ul style="list-style-type: none"> <li>OMB Circ. A-21, F. 6. b. (1)</li> </ul>	<p>A recharge center or service center is an internal operation that charges users for services or materials provided. Examples include: machine shop, glass blowing, animal care, recharge centers must use consistent and equitable cost accounting practices to ensure compliance with federal regulations. OMB Circular A-21 mandates that service center rates be:</p> <ul style="list-style-type: none"> <li>Based on actual or projected costs.</li> <li>Reviewed and recalculated periodically.</li> <li>Inclusive of all expenses related to the provision of service/product.</li> </ul>	<ul style="list-style-type: none"> <li>Recharge center charged more than total cost of providing the service/product (surplus).</li> <li>Recharge center billing rates not based on actual cost.</li> <li>All users not charged for services.</li> <li>Recharge center not billing all users consistently.</li> <li>Recharge center billing rates include unallowable costs in billing rates.</li> <li>Rates not reviewed periodically.</li> <li>Rates include cost of capital equipment.</li> </ul>
<b>Unallowable Costs</b>	<ul style="list-style-type: none"> <li>OMB Circ. A-21: C. 8.-9.; J</li> <li>OMB Circ. A122, A. 2.; A. 6.; B. 3.; Attach B</li> </ul>	<p>Which costs are unallowable; which costs should be refunded to grantor as unallowable costs; how to adjust previously negotiated F&amp;A cost rates containing unallowable costs; how to avoid the disallowance of costs due to disputes relating to cost unreasonableness or nonallocability.</p>	<ul style="list-style-type: none"> <li>Items charged to grants do not benefit the scope of work. Examples of these type of items might include: bottled water, coffee services, flowers, birthday cakes, books, ergonomic chairs, meals, general use computers, or software (MS Excel or MS Word).</li> </ul>
<b>Regulatory</b>			
<b>Animal Subjects Protections</b>	<ul style="list-style-type: none"> <li>NIH Grants Policy Statement, pp. 65-66</li> <li>Public Health Service Policy on Humane Care and Use of Laboratory Animals</li> <li>U.S. Government Principles for the Care and Utilization of Vertebrate Animals used in Testing, Research, and Training</li> <li>Animal Welfare Act</li> </ul>	<p>Universities that perform research on animal subjects are required to obtain the review and approval of the university's Institutional Animal Care and Use Committee (IACUC). University animal facilities are responsible for the compliant purchasing and supplying of research animals, the care of the research animals, and the fiscal management for animal related charges including purchase of animals (usage), husbandry services (per diem), and labor (i.e., surgical procedures).</p>	<ul style="list-style-type: none"> <li>Protocols for continuing research not reviewed and approved when required.</li> <li>Animal research taking place without protocol approval.</li> <li>Documentation of IACUC policies and procedures not sufficient.</li> <li>Animal charges not properly allocated to benefiting research projects.</li> <li>Animal per diem rates not representative of the actual cost.</li> </ul>

Compliance Requirement	Regulation	Summary	Related Risks
<b>Conflicts of Interest</b>	<ul style="list-style-type: none"> <li>• NIH Grants Policy Statement, pp. 44-46</li> <li>• 42 CFR Part 50</li> <li>• 21 CFR Part 54 Financial Disclosures by Clinical Investigators</li> <li>• Patient Protection and Affordable Care Act- Physician Payment Sunshine Provisions (Part A of the Title XI of SS Act section 1128G)</li> </ul>	The term “conflict of interest” refers to situations in which financial or other personal considerations may compromise, or have the appearance of compromising, an employee’s professional judgment with regard to the research they are conducting. Under 42 CFR Part 50, institutions must certify that they maintain a “written, enforced policy” on conflicting interests. Under the regulations, institutions must also report to NIH the existence of any conflicting interests and assure that the interest has been “managed, reduced, or eliminated.” The Sunshine Act requires applicable manufacturers to report research-related payments or other transfers of value that are ultimately made, in whole or in part, to covered recipients (e.g., physicians and teaching hospitals).	<ul style="list-style-type: none"> <li>• Institution does not have a conflict of interest policy or procedures.</li> <li>• Institution does not have effective procedures for reviewing the financial conflict of interest disclosures received from the investigators.</li> <li>• Institution does not properly maintain records of all financial disclosures and all actions taken by the Institution with respect to each conflicting interest for at least three years from the date of submission of final expenditures report.</li> <li>• Conflicts were not appropriately identified and communicated to the sponsor.</li> <li>• Conflicts were identified and communicated but were not properly managed.</li> </ul>
<b>Environmental Health and Safety</b>	<ul style="list-style-type: none"> <li>• NIH Grants Policy Statement, pp. 69; 145</li> <li>• The National Environmental Policy Act of 1969</li> </ul>	For construction grants, what policies/procedures are required relating to environmental health and safety.	<ul style="list-style-type: none"> <li>• Environmental health and safety.</li> <li>• Human and animal health and safety.</li> </ul>
<b>Export Controls</b>	<ul style="list-style-type: none"> <li>• 15 CFR Parts 700-799</li> <li>• 22 CFR Parts 120-130</li> <li>• U.S. Department of the Treasury, Office of Foreign Assets Control Sanctions Program and Country Summaries</li> <li>• Comments on regulations</li> </ul>	<p>Regulations that prohibit the sharing of certain information (e.g., military technology, technical data, trade secrets, etc.) with other countries and foreign nationals. Applies not only to disseminating information outside borders (e.g., shipping equipment, lecture in foreign country) but also to transferring knowledge to a foreign national in the United States (“deemed export”). Three government agencies regulate export controls:</p> <ul style="list-style-type: none"> <li>• State Department regulates military technologies via International Traffic in Arms Regulations (ITAR).</li> <li>• Commerce Department regulates non-military technologies via Export Administration Regulations (EAR).</li> <li>• Treasury Department bans or tightens controls on certain countries, including, Iran, Cuba, North Korea, Syria, and Sudan.</li> </ul>	<ul style="list-style-type: none"> <li>• Transferring equipment, technology, or something of value (could be physical or intellectual) that is export controlled without first applying for a license may carry significant penalties, including both civil and criminal, for the institution and the individual who ships the item.</li> <li>• Many universities contend that the majority of information shared during research, education, and other activities does not require an export control license because of the “Fundamental Research Exclusion” or “Education Exclusion.” These exclusions primarily impact “deemed exports.” Export controlled equipment and technology that is shipped outside the United States is NOT covered by these exclusions.</li> </ul>
<b>HIPAA Privacy and Security Laws</b>	<ul style="list-style-type: none"> <li>• 45 CFR Part 160</li> <li>• 45 CFR Part 164, Subparts A and E</li> <li>• 45 CFR Part 46, Subpart A, Basic HHS Policy for Protection of Human Subjects Protection</li> <li>• 21 CFR Parts 50 and 56</li> </ul>	Establishes national standards to protect individuals’ medical records and other personal health information. Requires appropriate safeguards to protect the privacy of personal health information, and sets limits on the uses and disclosures that may be made of such information without patient authorization. Also, gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.	<ul style="list-style-type: none"> <li>• Public exposure of PHI/PI.</li> <li>• Patients/subjects at risk for identity theft.</li> <li>• Patient/subjects medical condition may become know to a third party and may cause judgement or bias to patient.</li> <li>• Fines/penalties.</li> <li>• Negative publicity.</li> </ul>

© Huron Consulting Group Inc. All Rights Reserved.

Compliance Requirement	Regulation	Summary	Related Risks
<b>Human Subjects Protections</b>	<ul style="list-style-type: none"> <li>• NIH Grants Policy Statement; pp. 58-59</li> <li>• 45 CFR Part 46</li> <li>• Public Health Service Act</li> </ul>	University that performs research on human subjects is required to obtain the review and approval of the university's Institutional Review Board (IRB). The IRB approves the protocol, which is the outline or plan for use of an experimental procedure or experimental treatment. Review and approval must include all protocols involving humans, including externally and internally-funded research. Regulations are codified at 45 CFR Part 46.	<ul style="list-style-type: none"> <li>• Protocols for continuing research not reviewed and approved at least once per year.</li> <li>• Quorum is not present at meetings.</li> <li>• Mandatory training for key research personnel not performed.</li> <li>• Protocols for externally or internally funded research involving human subjects not reviewed.</li> <li>• Documentation of IRB policies and procedures not sufficient.</li> <li>• Informed consent forms confusing or unused.</li> <li>• Meeting minutes incomplete.</li> <li>• Inadequate HIPAA compliance.</li> <li>• Inadequate consideration of special populations (children, prisoners).</li> </ul>
<b>Invention Disclosures and Reporting</b>	<ul style="list-style-type: none"> <li>• 37 CFR Part 401</li> </ul>	What policies/procedures are required to comply with invention disclosure and reporting regulations.	<ul style="list-style-type: none"> <li>• Erroneous reporting and disclosures of invention.</li> </ul>
<b>Scientific Misconduct</b>	<ul style="list-style-type: none"> <li>• NIH Grants Policy Statement; pp. 50-51</li> <li>• Title 42 CFR Part 50, Subpart A</li> </ul>	<p>How to ensure that projects are not subject to research misconduct; what to do once research misconduct has either been alleged or determined to occur. Research misconduct does not include honest error or differences of opinion. 42 CFR 93* - Public Health Service Policies on Research Misconduct; Final Rule defines Research Misconduct as:</p> <ul style="list-style-type: none"> <li>• Fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results.</li> <li>• Fabrication: making up data or results and recording or reporting them.</li> <li>• Falsification: manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.</li> <li>• Plagiarism: the appropriation of another person's ideas, processes, results, or words without giving appropriate credit.</li> </ul>	<ul style="list-style-type: none"> <li>• Banned from future financial support for research.</li> <li>• Institution's lack of required assurance on file with ORI that states that the institution has written policies and procedures for responding to allegations of research misconduct and complies with its own policies and procedures. If the institution is too small to handle research misconduct process, ORI will work with the institution to implement a process for handling misconduct proceedings.</li> </ul>
<b>Scientific Overlap</b>	<ul style="list-style-type: none"> <li>• NIH Grants Policy Statement; pp. 32-33</li> </ul>	Scientific Overlap occurs when: (1) substantially the same research is proposed in more than one application or is submitted to two or more different funding sources for review and funding consideration, or (2) a specific research objective and the research design for accomplishing that objective are the same or closely related in two or more applications or awards, regardless of the funding source.	<ul style="list-style-type: none"> <li>• Duplicate work or redundancy.</li> </ul>
<b>Sub-Awardee Monitoring</b>	<ul style="list-style-type: none"> <li>• OMB Circ. A-110, .3; .22 (f) and (h)(2); .26(a); .29(c)</li> <li>• OMB Circ. A-122</li> </ul>	OMB Circular A-110 mandates that federal grant recipients monitor each program, function, or activity funded with federal grant awards – including sub awards. Sub recipient Monitoring is the process of providing oversight to sub awards throughout their lifecycle, including: obtaining the appropriate information prior to submitting the proposal (statement of intent, accurate budget, statement of work), reviewing appropriateness of sub awardee, executing an agreement consistent with A-133 requirements, and acquiring signed A-133 certification statements (from other A-133 institutions).	<ul style="list-style-type: none"> <li>• Lack of internal controls related to sub awards.</li> <li>• Lack of A-133 certification documentation.</li> <li>• Unallowable costs or lack of cost sharing documentation on sub awards.</li> </ul>

## Trusted Guidance

- ♦ Customized hospital solutions
  - ♦ Available 24 / 7
- ♦ Quality & compliance driven
- ♦ Proactive regulatory solutions



- ♦ Medical necessity
- ♦ Level of care
- ♦ Quality documentation
- ♦ Concurrent reviews
- ♦ Retrospective reviews
- ♦ Appeals

- ♦ Board certified, trained, & experienced physician advisors
  - ♦ Personalized customer service
  - ♦ State of the art systems & training
  - ♦ Strategic education for client staff

MedManagement, LLC  
205.970.8800

1500 Urban Center Drive, Suite 325  
1.866.298.1603

Birmingham, AL 35242  
[www.MedManagementLLC.com](http://www.MedManagementLLC.com)



# Establishing Processes to Document Medical Necessity: the Best Offense to Avoid Government Recoupments and Investigations

*Joan Ragsdale, Chief Executive Officer, MedManagement LLC.  
jragsdale@medmanagementllc.com*



## Introduction

**M**edicare, Medicaid, and other federal insurance programs (as well as private pay insurance programs) stipulate that payment for services will not be made unless the services are “reasonable and necessary” for the diagnosis or treatment of illness or injury. Providers certify that every claim submitted is medically necessary and have a legal obligation to provide clinical documentation supporting the medical necessity of treatments and services provided. Providers and payers agree and acknowledge that services must be medically necessary and reasonable for the patient and that there must be clinical documentation of both the services that were billed and the clinical need for the services.

## Medical Necessity Documentation

However, there is a widening gulf between the documentation required by auditors and payers for payment purposes and that which is prepared to ensure that there is adequate clinical documentation to demonstrate that necessary, quality services are delivered timely to patients. Recent activity by Recovery Auditors (formerly known as RACs), Medicare Administrative Contractors (MACs), Medicaid Investigative Contractors (MICs), Quality Improvement Contractors (QICs), and other federal and state recoupment and “fraud” investigation units have attempted (at times successfully) to impose documentation requirements beyond what providers traditionally provide in order to facilitate care to patients and to receive reimbursement for services. A five step approach to medical necessity documentation improvement efforts can help hospitals ensure that documentation supports the medical necessity of the services billed.

## Timely Documentation of Orders

First, hospital processes must ensure that orders are written and documented in a timely manner. If a physician writes an order for “inpatient services,” then the question is whether there is documentation to explain why inpatient services are appropriate in that particular setting for the specific patient’s condition at the time the order is written.

The physician is supposed to make a decision based on information available at the time of the decision. For a level of care decision (inpatient v. outpatient with observation services), inpatient status is only appropriate if the physician admits the patient because the physician determines that the patient is expected to need hospital care for twenty-four hours or more,<sup>1</sup> so the timing of the order becomes a critical factor in determining whether medical necessity documentation requirements are met. Hospital protocols must be designed to ensure that the entry of a correct order for bed placement is timely (made when the decision is made to place the patient in a bed) and that documentation supports the basis for the order.

Because level of care orders are written around the clock, there must be a process to review the orders, and their timing and documentation on a twenty-four hour basis, either through in-house case management and physician advisor services, or through outsourcing this functionality. Failure to conduct timely review can result in incorrect level of care determinations based on the severity of illness and treatment needs of the patient. Incorrect level of care determinations can negatively impact patients by inappropriately increasing the cost of care and jeopardizing their qualification for post-acute services. Incorrect level of care determinations can also negatively impact the hospital financially and compromise the facility’s quality measures.

<sup>1</sup> No text provided

### Detailed Documentation of Care Provided

Second, documentation must address “what” is being done for the patient. An order that reads “watch overnight” and “evaluate for discharge in the am” does not explain the specific services provided or why the services are being provided. Hospitals have tried to develop standardized order sets to ensure that important orders are not missed, but at best, the orders provide a glimpse into a care plan. At worst, standardized orders negate or minimize the physician’s assessment of the acuity of risk to the patient and the services needed to ensure a positive clinical outcome.

Hospitals should evaluate orders on a timely basis to ensure that the plan of care is documented when the patient is placed in a bed, and that the plan of care supports the level of care ordered (and to be billed). The documentation of timely orders is sometimes difficult for patients admitted from the emergency department. Accordingly, one area of focus for hospitals should be the timeliness of the institution in developing a care plan for each patient. Although it seems fundamental, it is not uncommon for the payment of hospital services to be denied because there is no documentation of what was done for the patient. Processes must ensure that orders for “what” is done is entered in a timely manner, and the service is delivered timely.

### Address the “Why” Question For Each Patient

Third, documentation must address the “why” question for each patient. Why does the patient need a service in a particular setting? For hospitals, the “why” question is generally a two pronged analysis: “Why does the patient need services in a hospital setting” and “Why does the patient need the services in the level of care setting that is ordered (inpatient v. outpatient).”

Medicare requires that physicians ordering services use “complex medical judgment” and consider a variety of factors that affect patient care and outcomes, such as the severity of the signs and symptoms exhibited by the patient, the medical predictability of adverse consequences, the need for diagnostic studies, and the availability of diagnostic tests at the time and the location where the patient presents.<sup>2</sup> Documentation must tell the story of why and how the patient presented, and why and what services are provided to address the needs of the patient.

The reviewers and auditors focus on Medicare guidance that services must be provided in the least intensive setting that allows the beneficiary to be treated safely without any significant and direct threat to the health of the patient. In the context of services rendered on an inpatient basis and observation services rendered to outpatients, the distinction between tests and treatment protocols may be minimal. It is important therefore to address the acuity of the risk that supports the expectation that the patient needs twenty four or more hours of hospital care. The

actual words are important, and documentation must be strong in all cases, but particularly in areas subject to intense scrutiny, such as one day stays. There must be a process in place to ensure that clinical documentation adequately tells the patient story.

In addition, there may be additional documentation requirements for the reimbursement of specific services. For example, inpatient rehabilitation or psychiatric inpatient services require admitting physicians to document why the setting is necessary to achieve clinical objectives. Similarly, certain local and national coverage determinations impose an obligation on providers to document failed outpatient therapies or approaches or provide additional documentation to demonstrate that a service is appropriate and meets reimbursement requirements.

In general, each hospital should ensure that there is a concurrent process in place to make certain that orders are timely, services are documented and the clinical documentation adequately explains why the service is appropriate and connects the dots for auditors. Whether internal or external physician advisors are utilized, there must be a process to ensure that documentation supports the services billed in each claim and provides adequate support for the rationale for the service.

### Continuity

Fourth, education and medical necessity documentation improvement must be continuous. As of this writing, there are two major proposed changes that would have a significant impact on case management responsibilities and documentation requirements for short hospital stays. Proposed Rule 1455 addresses re-billing opportunities where there is a level of care order that is not supported by documentation, and Proposed Rule 1522 addresses how CMS may define the 24 hour requirement.

In addition to regulatory changes, the areas targeted for review and interpretations of existing rules are constantly changing. Practicing physicians rely on knowledgeable case management and hospital staff to provide information on current documentation requirements.

Because physicians document for patient care purposes and not reimbursement purposes, hospitals must make an effort to partner with physicians to develop a collaborate approach to facilitate timely, compliant documentation.

Education should include case reviews from the facilities, review of specific documentation efforts, current guidelines, and inter-rater testing. Hospital leadership, including boards and executive leadership, need education about audit and recoupment initiatives and compliance challenges. Medical staff members and associates need to understand both the regulatory background and practical implementation approaches.

---

2 Medicare Benefit Policy Manual, Chapter 1.

### Integration With Audit Appeals and Clinical Quality Initiatives

Finally, medical necessity documentation efforts must be integrated with audit appeals work and clinical quality initiatives. What are the issues that have been identified by your MAC or QIC as problem areas? What aberrancies arise when a hospital's numbers are compared to peers? What issues have been identified through recoupments, and what processes, policies and education efforts have been implemented to ensure that issues are addressed?

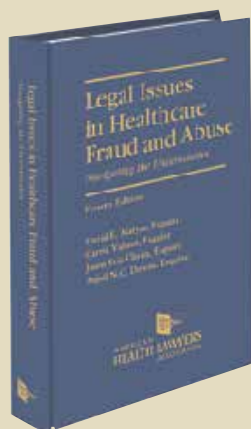
As pressures mount to increase scrutiny of payment for services, it is important that your case management team and your physician advisors work hand in glove to provide continuous feedback about processes. Just as compliance processes must be integrated into every aspect of patient care delivery

and employee communication, clinical documentation efforts must become the cornerstone of the care delivery processes. The investment in collaborative case management and physician advisor programs to foster communication with physicians at the same time that care is delivered is a wise investment that produces vast returns for both the hospital and the patients it serves.

Concurrent review of documentation may prevent significant loss of revenue attributable to inadequate documentation of services and rationale for services. It may also prevent recoupment or prepayment withholding, and ensure success if audited. Finally, it can create a culture of documentation compliance that will be necessary for hospitals to withstand increased efforts to scrutinize payment for medically appropriate services based on technical deficiencies. ♦

AHLA

## Check Out this Fraud and Compliance Title from AHLA!



*Legal Issues in Healthcare Fraud & Abuse, 4th Edition* is an excellent resource on healthcare fraud and abuse. It provides a thorough review of the major fraud and abuse laws, including the anti-kickback statute, the physicians self-referral prohibition (Stark), the False Claims Act, and the various administrative authorities.



For more information or to order, please visit  
[www.healthlawyers.org/bookstore](http://www.healthlawyers.org/bookstore)  
or call 800-533-1637.

# CLEAR IMPACT



Gain a comprehensive view of **dispute, compliance, and investigative** challenges with Navigant consultants who apply **targeted regulatory and industry expertise and practical insights** aimed at the healthcare industry.  
The result: **clear impact.**

NAVIGANT

[www.navigant.com](http://www.navigant.com)

DISPUTES & INVESTIGATIONS • ECONOMICS • FINANCIAL ADVISORY • MANAGEMENT CONSULTING

©2012 Navigant Consulting, Inc. All rights reserved. Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services. See [www.navigant.com/licensing](http://www.navigant.com/licensing) for a complete listing of private investigator licenses.



# Harnessing the Power of Data: A Primer for Health Care Attorneys

Mary Beth Edwards, Managing Director, Navigant,  
[mbedwards@navigant.com](mailto:mbedwards@navigant.com)

Bernard J. Ford, Managing Director, Navigant, [bjford@navigant.com](mailto:bjford@navigant.com)



## Introduction

The term “Big Data” has become ubiquitous. While social interactions and media in all their forms account for much of Big Data, few industries have seen a greater propagation of data over the last decade than health care. From drug and device development, to the proliferation of electronic health records (EHR), to the myriad of health claims submitted every day - we live in an age where we are inundated with data. Increasingly and inevitably, much of this data is being used against health care entities in litigation and investigations.

According to the most recent Annual Report issued jointly by the U.S. Department of Health and Human Services and the Department of Justice Health Care Fraud and Abuse Control Program, the government is continuing to enhance its data analysis capabilities and is increasingly relying on complex data analysis, predictive analytics, and data mining techniques to detect health care fraud and control health care spending.<sup>1</sup> Additionally, sophisticated *qui tam* relators have for many years used publicly available data to file lawsuits. Other relators have stolen data from their employers to make their claims. Regardless of the source, health care companies face many challenges from the use of their own data.

This article addresses several data-related topics of significance for health care attorneys who are defending companies enmeshed in litigation or investigations. Some of the topics may be relevant to attorneys who are counseling their clients on compliance or acquisitions, as well. The goal of this article is to help level the playing field by offering the knowledge gained over many years assisting counsel defending countless False Claims Act (FCA), Anti-Kickback, and commercial litigation matters.

## Investigations of Health Care Providers

The provider community is currently facing numerous investigations questioning the medical necessity of clinical services. These investigations seem to fall into two categories, the first raising questions about the propriety of an inpatient admission (i.e., site of service) and the second relating to whether a particular service was medically indicated (e.g., is a coronary vessel occluded to the point that a stent is required). “Medically necessary” is defined as a “term used by insurers to describe medical treatment that is appropriate and rendered in accordance with generally accepted standards of medical practice.”<sup>2</sup> As such, the determination of medical necessity is at the core of many of government’s activities.

According to the Centers for Medicare and Medicaid Services (CMS), an improper payment is a payment to the “wrong provider for the wrong services or in the wrong amount.” Such payments typically did not meet the statutory coverage requests, the medical necessity requirements, were incorrectly coded, or the provider did not submit sufficient documentation to justify payment.<sup>3</sup> Given the government enforcement efforts noted above, it is important that providers are cognizant of the power of data and data analytics and are able to utilize it, particularly when they are a target of an audit or an investigation, or are made aware of an allegation that requires them to assess their potential exposure.

Lack of medical necessity is identified as one of the major causes of improper payments and is a long-standing focus of government investigations, ranging from inpatient stays through long term care. According to the American Hospital Association,

1 The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2012. <http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2012.pdf> accessed on July 16, 2013.

2 Gillian I. Russell, FUNDAMENTALS OF HEALTH LAW 1, 25 (American Health Lawyers Association 5th ed., 2011). <http://www.healthlawyers.org/hlresources/Health%20Law%20Wiki/Medically%20Necessary.aspx> accessed on July 16, 2013.

3 Overview of Improper Payment Reviews Conducted by Medicare & Medicaid Review Contractors at [http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/CERT/downloads/Overview\\_Review.pdf](http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/CERT/downloads/Overview_Review.pdf) accessed on July 16, 2013.

RACTrac Survey for the Q1 of 2013, which tracks the Recovery Audit Contractors RAC activity, 96 percent of denied dollars were for the complex reviews, many of which focused on issues related to medical necessity. In fact, 68 percent of the reported medical necessity denials reported related to the short stay reviews, which focused on the appropriateness of the setting in which care was provided.<sup>4</sup> In those cases, the procedures performed were found to be medically necessary but the inpatient setting was found to be inappropriate.

These medical necessity denials occurred because the submitted medical documentation did not contain sufficient information to: 1) support the diagnosis, 2) justify the treatment/procedures, 3) document the course of care, 4) identify treatment/diagnostic test results, and 5) promote continuity of care among health care providers.<sup>5</sup> This information is generally captured and stored electronically as data in the EHR, however with some reviews going back farther (the proposed ten-year look-back rule), challenges relating to data stored only in hard copy or to data stored in limited capability, archived-only systems occur frequently.

Generally, when the government is investigating claims, it does so based on a limited set of data it initially collects for review but which does not always present an accurate representation of an error rate or overpayments. Thoughtful evaluation of the available data required to prove medical necessity can often significantly assist providers and their counsel in developing affirmative defenses and in evaluating the true error rate.

An investigation, an internal audit, or even an evaluation of government audit results will typically consist of several elements, each dealing with a different type of data.

» The first element is defining the population of interest (sampling frame) and creating a sampling plan by a statistical expert. An important factor in all reviews is the proper identification of the population of interest, which should start with evaluating each criterion for review in a way that excludes any irrelevant claims. This is perhaps more important when a review is conducted on a sample basis and not every claim is subject to an in-depth review. A statistically valid random sample is frequently utilized to conduct a review and a sampling plan is prepared, which includes defining sampling unit and a determination of an appropriate sample size. A replicable, random sample is then prepared.

» The next element is the evaluation of clinical issues and the determination of medical necessity by a clinician. If the review is conducted on a sample basis, the determination of medical necessity is done only for those randomly drawn sample claims. This requires

further gathering of data for these sample claims from a medical record including: assessments, treatment plans, physician orders, nursing notes, medication and treatment records, and other documentation, such as admission and discharge data and pharmacy records. It is important that the review be conducted by qualified personnel, typically a nurse or a physician, who are able to understand all the information contained in the medical record.

» The final element is the calculation of damages, including all mitigating offsets, by an analyst with reimbursement and data knowledge. In the case of short stay reviews, which focus on the appropriateness of the setting in which care was provided, claims that have been found during the review to be incorrectly billed as inpatient are those that are subject to damages. These claims are then re-priced using an Ambulatory Payment Classification APC grouper to reflect what the applicable Medicare payment would have been had the claim been billed and adjudicated as outpatient. In order to re-price the claim, additional data relating to detailed charges and payments and procedures coded with Current Procedure Terminology (CPT) on individual claims found to be subject to damages need to be collected. The re-pricing process frequently presents with data challenges; particularly if older claims are involved as they tend to be from the period prior to widespread institutional implementation of EHR and are frequently stored as paper-only copy or are stored in limited form in archives. If the review was conducted on a sample basis, the last step involves extrapolation of sample overpayments onto the population of interest.

The complexity of the provider reviews and the way data may be best used to assist in reviews is illustrated when the claims data (which ranges from simple identifying information such as admission and discharge data, through more complex information on diagnosis codes, procedure codes and CPT codes) is merged with medical record information used for the evaluation of sample claims, and with reimbursement-oriented information necessary to estimate payment error rate and calculate damage to create the smallest population of interest and design the appropriate sampling plan.

### Life Sciences Investigations

The TAP Pharmaceutical Products Inc. settlement in 2001 ushered in a period of numerous and significant investigations and settlements with pharmaceutical and medical device

4 American Hospital Association "Exploring the Impact of the RAC Program on Hospitals Nationwide" Results of AHA RACTrac Survey, 1st Quarter 2013, June 4, 2013 <http://www.aha.org/content/13/13q1ractracresults.pdf> accessed on July 16, 2013.

5 Recovery Audit Program (RAP) Demonstration High-Risk Medical Necessity Vulnerabilities for Inpatient Hospitals, ICN: 906269, Audio Date: 03/09/2011, [http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/SE1027\\_PodcastTranscript\\_ICN906269.pdf](http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/SE1027_PodcastTranscript_ICN906269.pdf) accessed on July 16, 2013.

manufacturers that continues to this day. From 2001 through mid-2012, the value of settlements related to investigations of pharma companies has totaled \$29.5 billion.<sup>6</sup> These investigations have been primarily focused on alleged kickbacks, off-label promotion, and foreign bribery and are very often data-intensive exercises. One issue that routinely arises when defending life sciences companies in FCA and Food Drug and Cosmetic Act matters is that damages are often predicated on reimbursements made by Federal health care programs for the company's products. While life sciences companies clearly know how much product they have sold (as well as the costs and profit of their products) they, unlike hospitals, doctors, and other health care providers, do not typically make claims directly to Federal health care programs. Consequently, they do not have claims data<sup>7</sup> at their disposal when and if they need to defend their actions during government investigations.

Off-label promotions are by far the most common target of government investigations of life sciences companies. Investigations of drugs that are reimbursed by Medicare Part D and Medicaid tend to be very different, and in some ways less complex, than those focused on drugs covered by Part B. Medicare Part B covers certain drugs that are administered by health care professionals outside of the hospital setting. Oncology agents, immunosuppressants, blood factors, and many other drugs are covered by Part B.<sup>8</sup> While many of the drugs covered by Part B have very specific therapeutic uses, many Part B drugs have been the subject of off-label investigations. Per unit reimbursement for these drugs can be fairly high, which is in part why historically, there has been a concern over the potential for misuse.

The most common data analysis challenges relating to Part B drugs involve the volume of claims implicated in an investigation, the conversion of package units to dosing units to billing units, and accurately evaluating the frequency of drug administration on a per patient basis. Even a modestly successful Part B drug may have several millions of dollars in claims that have been reimbursed by Federal programs during the time period covered by an investigation. When ancillary services necessary to administer the drug, or those that would not have been provided but for the administration of the drug, are factored into the equation, the total number of claims to be analyzed often more than doubles. Before analyzing data sets of this size, it is extremely important to evaluate the data carefully to completely understand any flaws that may have been created during the course of data extraction, and to appreciate the inclusion or exclusion of any fields that may harm or help the analysis. It is clearly a best practice to ask the government to provide the specific names of

the files/sources from which it extracts the data, the specific programming logic used to extract the data, and the control totals for the extract, so that when the data is uploaded for analysis the defense team can be certain they are using the correct data set.

Because many Part B drugs are solutions, they are administered via injections or infusions. Each drug has its own packaging requirements (single or multiple use vials), some come in multiple strengths, and each has its own Health Care Common Procedure Coding System (HCPCS) code used for billing purposes along with its unique National Drug Code (NDC). The units of measure for a package, a dose, and a billing unit may be different, may have changed during the time frame of the investigation, and may have been entered incorrectly on a claim. The combination of these issues requires careful analysis to make sure that the billing units at issue, which may be used to form the basis for damages, are accurately calculated. Misinterpretation of units (or perhaps worse yet, carelessness on the part of plaintiffs) can lead to significant controversy over damages.

Another challenge in analyzing large data sets of Part B drugs over multiple years arises when the company's defense hinges on the accurate assessment of patients' use of a drug over time. The drug's labeled indication requires use for a particular condition (acute v. chronic), the setting in which the drug is administered (the emergency department v. physician's office), and the frequency of its administration. The evaluation of longitudinal data hinges on the accuracy of each claim for a given patient. Experience has shown that claims data is far from perfect and in fact, may be confusing if not confounding. Claim fields that are prone to inaccuracies through time and can therefore have significant negative impacts on analyses are: principal and admitting diagnoses; units of service; UPINs; dates of service; and HCPCS/CPT codes. The identification of systemic errors related to these data fields is often impractical, if not impossible, as some can only be identified through the analysis of medical records. The analysis of these fields is quite important, particularly so anomalous data can be segregated and potentially excluded from causation and damages.

Life sciences companies have many other sources of data at their disposal, including drug-specific prescribing data purchased from vendors, data relating to requests for off-label information, sales call activity reports, and product sales and margin data. This data is typically either used defensively to prove a lack of causation or in the case of criminal matters, the sales and margin data may be used to compute exposures related to disgorgement of profits. Prescribing data from vendors comes in many forms from a variety of sources, including actual

6 From Appendix 2 of "Pharmaceutical Industry Criminal and Civil Penalties: An Update" dated September 27, 2012 published by the group Public Citizen. <http://www.citizen.org/documents/20731.pdf> accessed on July 16, 2013.

7 Claim is considered to be a request for payment submitted to Medicare or other health insurance. It is generally submitted on forms such as UB-04, UB-92, HCFA 1500, etc.

8 [http://www.cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra/Downloads/PartsBDCoverageSummaryTable\\_041806.pdf](http://www.cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra/Downloads/PartsBDCoverageSummaryTable_041806.pdf). Accessed on July 16, 2013. Please note that Medicaid frequently covers these same drugs and, consequently, when referring to Part B we generally include Medicare and Medicaid. Note further that these drugs may also be used in the hospital setting and appear on Part A claims but that the PPS doesn't typically pay for them separate and apart from the MS-DRG payment.

prescription data, surveys, and other sources. Care must be taken in analyzing this data not only because of the sheer quantity, especially for blockbuster drugs, but also the provenance of the data may not be fully-divulged by the data vendor for proprietary reasons. The use and analysis of data related to sales call activities and requests for off-label information must also be carefully considered. Many life sciences companies historically allowed sales reps to enter free form text in call notes; however, this practice has now been largely eliminated in favor of specified, drop-down entries in order to mitigate risks. Requests for off-label information have also become highly-structured at sophisticated life sciences companies and the systems used to house this data have reporting capabilities that allow for production and analysis.

## Pharmacy and PBM Matters

Pharmacies and Pharmacy Benefit Managers (PBM) face a number of complex disputes and investigations including FCA matters related to the dispensing and reimbursement of prescription drugs. Often these matters involve multiple, broad allegations based on vague examples and limited information and/or limited industry knowledge. These broad allegations may implicate a number of different client processes and operating entities, each process housing different types of data (e.g., dispensing data, accounts receivable, patient demographics) on disparate platforms. Thoughtful and holistic analysis of the client's data platforms can often provide a number of insights to help the company and counsel form defenses by allowing them to:

- » Develop a comprehensive analytical repository of all relevant data available to understand the transactions involved in the allegations
- » Collect specific evidence to rebut the example claims identified in complaints
- » Evaluate and confirm the positions taken by the client
- » Support discovery, by isolating the population of transactions at issue

One of the major obstacles encountered when a company faces broad allegations is that the accusations may involve a number of different business processes and operating entities. These various processes and entities may involve data stored on a number of disparate data platforms. Accordingly, any effective data analysis requires the ability to aggregate large amounts of data across a number of disparate platforms into one analytical data repository.

Ensuring that the data from each of the different platforms can be integrated into one comprehensive data repository requires in-depth knowledge of the various company processes from both an industry and technical perspective. This requires counsel and consultants to meet with the client's subject matter experts (operations and IT) for each of the platforms to

thoroughly understand how the data was stored, how it is used in conducting the company's business, and how it could relate to other data platforms.

The aggregated data can provide a number of benefits to the company and counsel by allowing the company to tell the full story of example claims, disproving many of the allegations, ensuring consistency with the company's positions and policies, leveraging the knowledge gathered to educate 30(b)(6) witnesses, and minimizing the number of witnesses needed to litigate the case.

One of the key challenges an organization may face is that the plaintiff/relator often bases the complaint on data mined from within that organization. The plaintiff/relator will include examples of claims submitted by the organization that appear to support the allegations. However, the organization will have access to much more extensive data regarding each transaction than the opposing side, which can be leveraged to dispute the relator's claims. For example, a client can aggregate data from the main claims repository, supplemental patient demographic data, accounts receivable systems, and PDE data. Reports can then be constructed from this aggregated data to reflect all the relevant data for each of the sample claims submitted by the relator and contradict the limited data in relator's possession. This is a powerful exercise to demonstrate that the relator's evidence is either factually inaccurate or is not representative of a systemic weakness in the organization.

Another important use of data to defend against fraud allegations is to confirm that the actual experience is consistent with the organization's position and policies. For example, the organization may indicate that certain pricing arrangements reflect fair market value. Data analytics can be used to review client's inventory and purchasing data, and compare it to the claims experience and customer contracts to determine whether the prices appear to reflect fair market value.

The results of these analyses can help to disprove allegations or isolate specific areas of risk to focus on (e.g., specific locations, individuals, drugs, or processes) for further analysis and detailed review. In addition, these analyses can ensure that an organization can counsel and put forth arguments that are supported by the actual experience of the company.

Another key aspect to representing a client in these matters is supporting discovery. When responding to discovery requests, it is important to identify the relevant data that needs to be produced in response to a particular request. The ability to successfully isolate the specific transactions and corresponding data relevant to a dispute (or, more importantly, exclude what is not a relevant data) is a critical piece of the process. An in-depth analysis of the data available can identify transactions that are outside of time periods of interest, not associated with the relevant geographic areas, or are not applicable to certain disputed agreements with other payers. These steps are vital to limiting the client's exposure and minimizing the risk that the plaintiff/relator will access additional data that could be used to expand the scope of the claims.



## Payment Disputes Affecting Payers

Payers of health care claims confront numerous complex challenges from many directions regarding claims reimbursement. Disputes can arise from a group of providers or members contesting the interpretation of reimbursement terms included in network agreements, alleging the misapplication of a particular fee schedule, or contesting the reasonableness of a payer's "usual and customary" reimbursement. Regardless of the nature of the dispute, they often involve large volumes of complex health care claims. Thoughtful analysis of the data available can often significantly assist payers and their counsel in quantifying the financial impact of the issue and in developing affirmative defenses. A few examples of the many ways data analysis can impact these disputes include:

- » Isolating the Relevant Claims: Whether initially identifying responsive data for a discovery production or calculating potential damages, the ability to successfully isolate health care claims relevant to a dispute (or exclude those claims not relevant) is a critical piece of the process. An in-depth analysis of the data available can identify claims outside of the parameters of the dispute so that damages are limited to the relevant claims. Data parameters that are frequently subject to isolation or removal in payment disputes include: dates of service, product lines, funding arrangements and/or denials (e.g., duplicates, member not eligible). Isolating the data to the relevant claims in dispute ensures that the scope of the case is not unintentionally or inappropriately broadened.
- » Sizing the Dispute: Contract disputes with payers often center on a disagreement regarding the application of particular terms included in an agreement, frequently related to reimbursement. Attempting to estimate the potential exposure under the terms of the contract can be difficult without a thorough understanding of the data underlying the dispute. Data

analysis can identify the volume and types of services at issue to help counsel and clients prioritize their arguments and research. Additionally, data analysis can quantify potential exposure under a variety of scenarios, by re-pricing claims under different interpretations of the disputed terms, and providing payers and their counsel with a range of exposure they may face.

Some payment disputes involve allegations of process controls errors. Electronic data can play a key part in evaluating the existence of these errors and estimating the potential exposure. Payers frequently face allegations of process control errors based on limited or inaccurate sampling by the government or the opposing party. Data analysis can be used to demonstrate that the purported errors found in the sample are not representative of the universe of claims adjudicated by the payer. Analyses that can help clients and counsel address sampling weaknesses include: validating whether the sample was drawn from the appropriate universe of claims, whether the sampling unit was determined correctly for the relevant claims, whether the sample size was sufficient, and whether extrapolation was correct. When large volumes of claims are processed, errors in the application of sample design can expose payers to unnecessarily large liability which can be mitigated by an effective analysis of the electronic data.

Data is also used to demonstrate that the errors alleged in a dispute are not systemic. When a payer faces allegations of process control failures, it is important to understand the frequency and magnitude of these occurrences to defend against the claims. Analysis of electronic data, which may include a combination of claims, eligibility, provider and medical management systems, can isolate the instances, if any, in which the alleged errors were occurring, allowing counsel to prioritize the focus of its investigation and evaluate potential exposure.

*The authors acknowledge and thank the following colleagues for their valuable contributions to this article: Urszula Zapolska, Diane O'Hara Folckemmer, Jed Smith, Matt Ryan and Jeremiah Sinclair.*



# BALANCING RISK AND DEFENSIBILITY



Learn more about our  
services and products at  
[WeArePendulum.com](http://WeArePendulum.com)!

Pendulum helps our clients in a variety of healthcare settings minimize professional liability exposure by balancing risk and defensibility.

Pendulum provides many risk management services and products:

- On location professional liability assessments, OIG compliance assessments, customer service assessments, one-day focused regulatory survey reviews, security vulnerability assessments, mock OSHA assessments, disaster preparedness assessments, and more
- Desk-based professional liability assessments
- Web-based incident reporting
- PL/GL claims processing service
- Social media listening (facility, trial, and jury monitoring)
- Pendulum online Risk Management Resource Center
- Specialized risk management tools

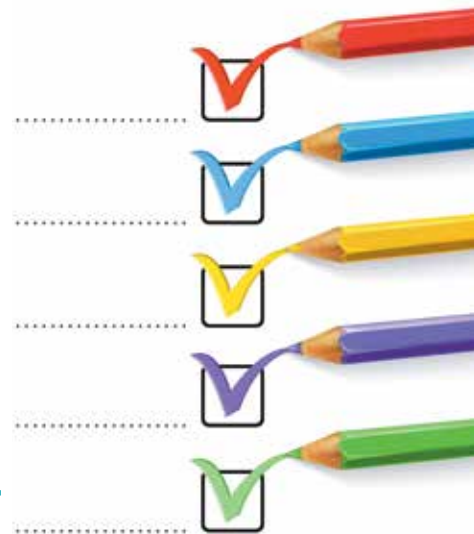
[www.WeArePendulum.com](http://www.WeArePendulum.com) • 888-815-8250

[info@WeArePendulum.com](mailto:info@WeArePendulum.com)



# Striving for Quality & Staying in Compliance: A Continuous Challenge for Long Term Care Facilities

*Kathleen A. Hessler, RN, JD, Independent Risk Control Consultant, Pendulum, LLC, [khesslerlaw@comcast.net](mailto:khesslerlaw@comcast.net)*



## Introduction

“Does your facility have an active compliance program?” I ask as I sit down with the administrator of a skilled nursing facility (SNF). I am on assignment to conduct a one-day risk assessment on behalf of Pendulum LLC, a healthcare risk management firm specializing in on-site assessments and other loss control services.

“No,” the administrator says. Sometimes the answer is short and simple; sometimes the question is met with a blank stare. A confident administrator might say “Yes, of course. We follow HIPAA rules, and we only had three minor deficiencies in our last Medicare survey.”

When it was signed into law in 2010, the Affordable Care Act (ACA) created a requirement that all Medicare-certified SNFs have a viable compliance and ethics program in place effective March 23, 2013.<sup>1</sup> However, many nursing home management personnel are not aware of this requirement. Additionally, many facilities are not aware of the Department of Health and Human Services (HHS) Office of Inspector General (OIG) Compliance Program Guidance (CPG) that was originally published as a voluntary guidance in the Federal Register in 2000<sup>2</sup> and supplemented in the Federal Register in 2008.<sup>3</sup>

Although CMS has not yet drafted or implemented enforcement regulations regarding compliance program requirements, SNFs who may have missed the March 23, 2013 deadline should begin, if they have not already, to implement a facility- or company-wide compliance program. There may be a grace period for facilities that have not yet complied due to the lack of published

enforcement regulations. However, CPG for SNFs has been around for more than a decade, and CMS may not deal kindly with facilities that do not have a program in place.

While many large national companies have corporate compliance programs in place and their facilities are aware of the need for such plans, some facility management teams do not fully understand the rationale for such programs. Specifically, there is a lack of knowledge and understanding about the OIG’s major initiative in the late 1990s urging healthcare providers to voluntarily implement compliance measures in an effort to prevent the submission of erroneous claims and to combat civil and criminal fraud and abuse. Although most facilities have some compliance measures in place as listed in the OIG CPG, many do not have a fully developed compliance program.

The OIG is serious and active in investigating and prosecuting civil and criminal fraud and abuse in healthcare, including SNFs, as evidenced by the many enforcement actions and judicial proceedings that have occurred over the past decade. Yet to many administrators and others in SNF management positions, the compliance program requirement is just one more legal mandate to overcome.

During my more than 20-year career as an attorney, risk manager, compliance officer, and consultant (with a special focus on long term care), I have encountered more than a few discouraged facility management personnel. The reach of state and federal regulations; constant surveys; simultaneous, multiple-agency investigations; allegations of malpractice and wrongful death; and the government compliance program mandate have exhausted the most competent managers. While these regulatory requirements

<sup>1</sup> See Section 6102 of the ACA.

<sup>2</sup> 65 Fed. Reg. 14269.

<sup>3</sup> 73 Fed. Reg. 56832.

can be beneficial, many facilities become discouraged and overwhelmed because they do not believe they have the necessary resources to develop, implement, and maintain these programs.

This article will provide some basic recommendations for structuring a compliance and ethics program that works with the nursing home's quality assurance and performance improvement plan so that there is minimal redundancy in staff activities. Just as oil and vinegar combine to provide a desirable flavor, these two programs, when appropriately mixed, can work together to form effective and rewarding facility- or company-wide programs. Still, a compliance program ultimately should be the stronger monitoring and auditing arm of a facility. Like oil and vinegar, there will always be separation of the two.

This article will also show that many facilities already have elements of a compliance program in place and will provide examples on how established facility practices can be strengthened to meet both compliance and other regulatory needs without duplication of elements and practices.

### Overview of OIG Compliance Guidance Elements

As noted above, in 2000, the OIG published the first seven elements of an effective compliance program, stating that the governing body of a nursing facility should firmly establish its commitment to them; the 2008 supplemental CPG provided an eighth element. Specifically, the OIG recommends that SNFs implement the following measures as elements of their compliance program:

1. Establish written standards of conduct and policies and procedures that demonstrate the facility's/company's commitment to compliance
2. Designate a compliance officer and appropriate committee(s) charged with the responsibility for the program
3. Develop and implement regular and effective education and training programs for employees, contractors, and vendors
4. Create and maintain effective lines of communication between the compliance officer and employees, including a hotline or other reporting procedures protecting the anonymity of any reporters
5. Develop and implement training materials for the staff, contractors, and vendors on disciplinary actions for violations of policy and law
6. Monitor high-risk areas through use of auditing and risk management techniques to identify problems
7. Provide prompt investigations of identified issues and proper response to detected offenses and initiate corrective actions, including repayments and preventive measures
8. Provide regular review of compliance program effectiveness

Additionally, the 2008 supplemental guidance includes recommendations and discussions on identified risk areas, such as

quality of care, submission of accurate claims, and the federal Anti-Kickback Statute. The OIG also lists areas of special focus, including quality of care delivery (sufficient staffing, comprehensive resident care plans, medication management, appropriate use of psychotropic medications, etc.). Resident safety is also a special risk area and encompasses resident interactions and staff screening.

Each year, the OIG publishes its annual *Work Plan*, which lists several specific areas of focus that the OIG will target during a calendar year. For instance, in 2013, the OIG *Work Plan* identifies adverse events and temporary harm in post-acute care in SNFs as a focus of review. The OIG will also focus on how SNFs address certain federal requirements related to quality of care and to what extent SNFs use Residential Assessment Instruments (RAI) to develop care plans.

As SNF billing and payments are currently tied to resident assessments, services received, and quality of care delivery, facilities may find themselves in harm's way if they do not have an active quality assurance/performance improvement program as well as an effective monitoring plan through which the compliance officer and compliance committee can audit, identify, and correct problems. Specific problem areas that should be reviewed include resident record documentation (including care planning) and coding and billing documents (including Minimum Data Set).

### Striving for Quality

Since the implementation of the Omnibus Budget Reconciliation Act (OBRA) in 1987, all skilled nursing facilities have been required to create and maintain a quality assurance program. Regulation 42 CFR, Part 483.75 (o) specifies that facilities maintain a quality assessment and assurance committee. Additionally, the regulation, also known as F-Tag 520 in the Medicare State Operations Manual for Skilled Nursing Facilities, provides that the membership of the committee include, but not be limited to, the medical director and the director of nursing. A facility is directed to conduct quarterly meetings (at a minimum). The regulation further states that the quality committee "develops and implements appropriate plans of action to correct identified quality deficiencies."

Because of this long-standing regulation, most SNFs have acceptable quality assessment and assurance programs; some even have stellar ones. However, a facility's quality program is not always effective in identifying process problems and system improvements. For instance, while many facilities collect data in such areas as resident falls, pressure ulcers, medication errors, and infections, too many of them do not fully understand the purpose of tracking and trending this data—they miss opportunities to analyze the data and detect specific patterns or systemic problems that need correction. This is especially true if facilities do not use computerized event systems or dashboards for data analysis. In essence, some facilities may be going through the motions, reporting data at quality assessment and assurance committee meetings but not using the information effectively to



identify specific problem areas. Therefore these facilities are not initiating performance improvement plans, assigning accountability, and engaging in follow-up monitoring.

Recognizing this as a concern, in recent years CMS has focused on quality assessment and assurance programs during its survey process. Additionally, Section 6102(c) of the ACA requires HHS to establish and implement a quality assurance and performance improvement (QAPI) program for SNFs. Under the QAPI program, HHS is charged with establishing standards relating to QAPI with respect to facilities. Further, HHS must provide technical assistance to facilities on the development of best practices to meet such standards. And finally, HHS must promulgate regulations to meet the requirements of the statute. To that end, after a SNF demonstration QAPI program was launched in fall 2011, CMS had sufficient feedback to develop materials and publish guidance and tools to assist facilities in developing an effective QAPI program.<sup>4</sup>

While a facility's existing quality assurance program may be the foundation for its QAPI plan, management staff should look to and study the CMS tools and guidance in an effort to fully integrate performance improvement activities into its current quality assurance program. By doing so, management will be able to establish the necessary practices and analyses to detect problems, develop actions plans, assign accountability, and provide follow-up monitoring. These activities will allow the facility to involve all members of the organization in identifying opportunities for improvements. Finally, a facility will be able to establish systems to allow for monitoring the effectiveness of corrective actions. In sum, by utilizing a fully functioning QAPI program, a facility will be able to recognize gaps in systems or processes.

If a facility's QAPI committee develops and implements best practices, it sets the stage for the compliance officer and compliance committee to audit the high-risk areas in which the facility is collecting data. If the two committees work together, but also independently, toward the same goal, the facility can strengthen the quality of its services. The compliance committee can, in turn, develop and offer auditing protocols and monitoring activities. Together these committees can identify problems and implement successful improvement actions. The compliance officer or a member of the compliance committee should sit on the QAPI committee for clarity of purpose and successful integration of monitoring improvement plans.

## Stay the Course for Compliance

### Compliance Officer and Plan

One of the OIG's stated purposes for creating a corporate compliance and ethics program is to prevent billing errors as well as civil and criminal fraud and abuse. Since billing and reimbursement in SNFs are tied directly to the level and quality of services provided, it is in the facility's best interests for its quality assurance and performance improvement committee or

subcommittee(s) to work in collaboration with the company's compliance program committee.

Once a facility takes the initial steps in implementing a compliance program by appointing a compliance officer and establishing a compliance committee, drafting a program document complete with key policies, procedures, and a company/facility code of conduct is the next order of business.

### Code of Conduct and Policies and Procedures

A facility or company should first look to existing policies and procedures and its employee handbook to determine if any policies and procedures currently in place are applicable to a code of conduct. Many companies may already have a code of conduct that addresses resident rights, safety issues, anti-kickback concerns, conflicts of interest, drug testing, resident abuse, background checks, progressive discipline, etc. If the facility already has a code of conduct, it may need updating or revising to better fit the needs of the compliance program.

A specific code of conduct may need to be developed, however, and for some facilities, it may be appropriate to include it in the employee handbook. However, it is important to keep in mind that the code of conduct should also apply to board members, vendors, and independent contractors with whom a facility does business. If there is already an applicable code of conduct in the employee handbook, a facility may wish to use existing language to develop a separate document for all vendors and independent contractors.

Alternatively, a facility may decide to separate the code of conduct from the employee handbook and strongly communicate to staff that the code goes to the heart of the facility's compliance program. There is no "one-size-fits-all" compliance program; as such, facility management should determine what design best meets its needs.

A robust compliance program should include policies and procedures that address the following: contract review, employee background checks, compliance training and education, anti-retaliation, discipline for and reporting of violations, billing and coding, record retention, regulatory inquiries and investigations, accounting and financial reporting, auditing and monitoring activities, and annual identification of risk areas. (Note that this list of suggested policies is not all-inclusive.)

A facility may cross-reference manuals if a particular policy is included in more than one program or manual. Having two different policies on the same matter should be avoided, as it may create confusion and cause inconsistencies in application. However, all policies and procedures should be reviewed annually to ensure they meet best practices and current regulatory standards.

### Training and Education

Policies and procedures are only as good as the employees' knowledge and understanding of the documents. Therefore, a facility should develop training and educational materials

<sup>4</sup> See CMS Web site at [www.CMS.gov](http://www.CMS.gov) and search "QAPI."

that not only cover compliance program education but provide training on all high-risk areas included in compliance program documents. Some education programs can be given to all staff, while others can be provided only to a specialized audience. For instance, the business office manager and Minimum Data Set coordinator should have special education on Medicare/Medicaid requirements, including billing and coding, and nursing staff should receive ongoing education and in-servicing on medication management and psychotropic medication administration, monitoring, and documentation. All direct caregivers should be educated on the value of an individualized care-planning process and the active use of care plans.

In accordance with regulations, most facilities have strong systems in place that provide for certain mandated educational programs during orientation and on an annual basis. These programs include but are not limited to HIPAA, abuse, infection control, resident rights, and safety. Compliance training can be added to employee orientation and to the mandatory annual training for all staff. Furthermore, specialized programs should be incorporated as indicated by compliance program documents. Records of training materials and sign-in sheets confirming attendance and understanding of materials, preferably through tests, should be maintained in files per the facility's record-retention policy.

#### **Communications/Hotline**

Communicating and reporting concerns and actual violations of policy or the law is imperative to an effective compliance program. Many organizations use an anonymous reporting system, such as a hotline, but other systems may be implemented as well.

#### **Disciplinary Standards**

Many facilities have employee policies that address progressive disciplinary standards. However, depending on a facility's existing policies, it may be necessary to enhance the standards to address violations of civil and criminal law. Additionally, the compliance committee should consider auditing and monitoring employee files in real time to ensure that documentation reflects accurate practices for progressive discipline.

#### **Monitoring and Auditing**

As previously discussed, many facilities collect and analyze data to identify system issues or problems that need corrective actions. These are the first steps in the monitoring and auditing functions. However, other auditing activities may include review of human resources files to ensure compliance with criminal background checks, the OIG exclusion list, drug screening, sex offender registry checks, and reference checks, to name a few. The compliance committee may conduct systematic auditing of medical records, with a focus on review of resident records for timely individualized care plans and documentation of psychotropic medication management, including reduction or a clear explanation of why reduction was not indicated.

Additionally, the compliance committee may develop and use audit forms that are specifically designed for high risk areas.

Alternatively, the committee may engage external auditors for annual audits of billing and cost reports. Other areas of review may include contract compliance with anti-kickback laws. Results of audits can be reported to the QAPI committee or various subcommittees; the committees then will be able to develop and implement action plans that address areas of need as identified by the audit process.

#### **Prompt Investigation and Reporting**

The compliance officer should conduct prompt investigations once aware of allegations of illegal activities or violations of policy. The results of these investigations should be reported in a timely and appropriate manner through the facility's chain of command, governing board, and government agencies per the facility's compliance policy regarding investigating and reporting.

#### **Annual Updates and Reassessment of Program**

The compliance officer and committee should annually review the *OIG Work Plan*, remain current on CMS mandates and OIG's targeted areas of focus, and consider developing annual quality initiatives in partnership with the QAPI committee.

#### **Integrating Quality and Compliance Programs**

Facilities need efficiency without duplication of elements and practices. But with multiple government regulations, it can be difficult to sift through program requirements and develop the necessary infrastructure without creating redundancy.

However, if facilities take stock of current QAPI functions and other facility activities, they should find that they perform many QAPI and compliance functions on a daily basis. If QAPI and compliance activities are viewed as an integrated way of providing services to achieve quality of care and quality of life for residents, a facility is more likely to be in compliance with ethical standards and regulations. By focusing on the whole system, management staff may feel less overwhelmed and feel a sense of accomplishment.

For instance, some facilities conduct daily stand-up committee meetings which are attended by all department heads. Areas of discussion may include current incidents, residents at risk for falls or elopement, Medicare residents, survey issues, and review of fire or hazard drills. Some facilities choose to call these meetings their "daily QAPI meeting," "quick QA quips," "morning meeting," or "daily huddle." Whatever the nomenclature, these daily meetings cover many issues related to quality and compliance, and they can spotlight a facility's weaknesses, such as a lack of firm action plans, accountable personnel, and follow-up monitoring.

Some facilities form subcommittees of their QAPI committee and involve additional staff who work with the committee. These subcommittees may focus on clinical risk areas such as a falls program, pressure ulcer prevention, billing and Minimum Data Set coding accuracy, safety issues, etc. These subcommittees meet on a routine basis to determine what areas may need a process improvement plan. The compliance committee can work with these subcommittees to assist with the development of action plans and auditing of system changes.



A facility may consider these committees part and parcel of its QA program. In other words, the QAPI program is the umbrella under which staff, through the daily meetings and the subcommittees, perform process improvement work. In essence, through these meetings, the staff is striving for quality through timely reviews, investigations, and development of action plans to correct identified issues. This information can then be reviewed in monthly or quarterly QAPI committee meetings.

### Conclusion

Since the OBRA regulations were signed into law in 1987, long term care professionals have confronted numerous CMS regulations, revisions, and an increasing number of new enforcement initiatives. State Departments of Health strenuously survey facilities per their (Department of Health) contract with CMS. Additionally, facilities may be visited by their state's ombudsman programs, departments on aging, and adult protective services, all conducting independent investigations. Finally, in the past

decade, SNFs have seen an increase in the number of civil and criminal investigations conducted by state attorney general offices, the OIG, and the federal Department of Justice.

There is no question that facility administrators and directors of nursing are continuously under the microscope to ensure compliance with state and federal regulations, all in an effort to provide quality of care and quality of life for SNF residents. The burden of these demands may be lessened if management annually reviews existing policies, procedures, and current practices; enhances them as necessary; and develops and follows systematic, consistent approaches to training, education, auditing, and monitoring. Management should view its QAPI plan and compliance program as vital and integrated mechanisms that can help the facility provide quality care and ensure regulatory compliance. ♦

*This article is for education purposes only and should not be construed as legal advice.*

**AHLA**

## Check Out this Fraud and Compliance Title from AHLA!



*Pharmaceutical and Medical Device Compliance Manual* offers an in-depth overview of the federal and state enforcement agencies that are responsible for investigating and resolving violations of the law by healthcare entities, with an emphasis on pharmaceutical and medical device companies.

For more information or to order, please visit  
[www.healthlawyers.org/bookstore](http://www.healthlawyers.org/bookstore)  
or call 800-533-1637.



**VISION  
BEYOND**  
the Numbers®



## Be Ready.

**Compliance demands aren't  
always easy to predict.**

In today's regulatory environment, it isn't easy to meet compliance demands. PYA professionals can assist you in developing an effective compliance program and in implementing a successful work plan for the future.

And, when the forecast changes, we also provide assistance with investigation and remediation.

**We call it Vision Beyond the Numbers,  
and it can work for you.**



**VISION** » Hospital & Physician Compliance | Medicare & Medicaid Compliance | Anti-Kickback, Stark, False Claims Act Compliance

[www.pyapc.com](http://www.pyapc.com)

# Demonstrating Compliance Program Effectiveness in an Ever-Changing Healthcare World

*Martie Ross, Principal, Pershing Yoakley & Associates, [mross@pyapc.com](mailto:mross@pyapc.com)  
Marjorie Scott, Manager, Pershing Yoakley & Associates,  
[mscott@pyapc.com](mailto:mscott@pyapc.com)*



## Introduction

In an increasingly complex and integrated healthcare industry, the challenge to maintain a comprehensive, effective compliance program within a healthcare entity continues to test even the most sophisticated organizations. The breadth of issues to be considered, decentralized nature of patient care, and frenetic pace of affiliation amongst healthcare entities all hold the potential for compliance missteps or oversights. As healthcare organizations continue to evolve, the task of building and/or maintaining a compliance program becomes even more challenging. Boards of Directors, C-Suite executives, management teams, and others often find out too late that the current compliance program is inadequate, as they scramble to decide how to bring it back into focus and make it effective as quickly as possible.

The starting point for organizing and continually keeping a healthcare compliance program effective, for hospitals, physician groups and other healthcare entities, is the U.S. Department of Health and Human Services Office of Inspector General's (OIG) series of compliance program guidance documents.<sup>1</sup> Any experienced compliance officer can recite the seven elements recommended by the OIG for an effective compliance program:

1. Designate a compliance officer.
2. Implement written standards with policies and procedures.
3. Provide staff training and education.
4. Develop open lines of communication.
5. Conduct internal audits.
6. Respond to wrongdoing with remedial and proactive measures.
7. Enforce disciplinary standards.

Merely having a written compliance plan that addresses each element of the compliance program, however, is not sufficient. Enforcement authorities expect a provider to present objective proof of the compliance program's effectiveness in detecting, preventing, and correcting corporate wrongdoing:

**"Prosecutors should...attempt to determine whether a corporation's compliance program is merely a 'paper program' or whether it was designed, implemented, reviewed, and revised, as appropriate in an effective manner."**

Additionally, authorities expect providers to engage in thorough and regular reviews of their compliance programs to identify and correct any impediments to effectiveness:

**"Hospitals should regularly review the implementation and execution of their compliance program elements. This review should be conducted at least annually and should include an assessment of each of the basic elements individually, as well as the overall success of the program. This review should help the hospital identify any weaknesses in its compliance program and implement appropriate changes."<sup>2</sup>**

Recently, some healthcare facilities have chosen to reduce or put their compliance program on hold in order to provide immediate financial relief amidst cost reductions and budget constraints. Unfortunately, this delay only increases the risk of falling into a downward spiral or returning to a previous situation in which the organization may have had untenable compliance risk exposure. Social media and regulatory pressures continuously remind organizations of the negative consequences of not adhering to daily compliance initiatives, which are ultimately reflected in their operations.

<sup>1</sup> The complete set of OIG's compliance guidance documents is available at <https://oig.hhs.gov/compliance/compliance-guidance/index.asp>.

<sup>2</sup> OIG Supplemental Compliance Program Guidance for Hospitals, 70 Federal Register 4858 (January 31, 2005). This document is available at <http://oig.hhs.gov/fraud/docs/complianceguidance/012705HospSupplementalGuidance.pdf>.

The OIG has not given specific directions regarding the scope and structure of compliance program audits; however, the OIG has provided enough guidance for healthcare facilities to produce an effective compliance program and document the results of compliance program testing. Despite the guidance offered by the OIG, the absence of specific guidance language has resulted in hesitancy among some providers to invest the time and resources into such formal reviews. Their inaction does not necessarily reflect a lack of commitment to compliance, but rather a lack of clear understanding on how to demonstrate program effectiveness. Regardless of the entity's reasoning, their inaction is likely placing their organization at greater risk of a compliance violation.

In order to implement a strong compliance program, it is imperative to understand the framework of compliance standards outlined by the OIG. Analysis of the OIG's compliance guidance documents, as well as formal corporate integrity agreements<sup>3</sup> and various resources and educational materials produced by the OIG,<sup>4</sup> has identified three standards by which to evaluate and improve compliance program effectiveness – **structure**, **substance**, and **commitment**.

### Structure

Just as contractors follow, and inspectors apply, building codes, providers and their auditors should employ a “compliance code” derived from the Federal Sentencing Guidelines for Organizations<sup>5</sup> and the aforementioned OIG pronouncements on the subject. While billing audits focus on medical record documentation, a review of a compliance program's structure must be comprehensive and ensure regular review of many other documents and processes, including but not limited to:

- » governance documents, board minutes, policies and procedures
- » job descriptions
- » compliance committee agendas and minutes
- » compliance-related inquiries (receipt and response)
- » reports of possible compliance-related issues (receipt, investigation, and response)
- » audit plans and reports
- » documents relating to compliance training and program promotion

For any size organization, all training materials should be saved and be readily available for presentation should an audit occur. Compliance program training materials and evidence of employee participation and knowledge of the compliance program



may include: videos; in-person presentations; PowerPoint slides; and participant tests or quizzes to reflect employees' level of understanding, competency, etc. In addition to the results of the participants' tests and quizzes, a detailed log of the employees' information, including names, identification numbers, dates and times of the education or training should also be maintained. Finally, the documentation should specify the secure location where the materials are saved.

For health systems, the compliance program review of structure should include an evaluation of the program's ability to operate effectively at all organizational levels, i.e., at the system level as well as at individual facilities. For example, a local facility employee may be unlikely to report a compliance concern to someone he or she never has met at the central office. In some cases, system-wide compliance officers may find it difficult to become familiar enough with a distant facility to conduct an effective investigation.

At the same time, however, all system employees should be held equally accountable to the same organizational standards of ethics and compliance. In order to do this effectively, the compliance department must devote the time and resources necessary to communicate and educate its personnel. In turn, employees should have confidence in their employer and know that when they report an incident or concern that it will be handled and addressed in an appropriate manner every time.

### Substance

Many compliance programs suffer from the lack of a clearly defined role within the organizations they serve. A compliance program audit should include a detailed analysis of the program's current scope of services, including its relationship to other key organizational functions (e.g., risk management, human resources, provider contracting, billing, health information management), as well as the substantive areas within the program's

3 The corporate integrity agreements into which the OIG has entered with healthcare providers as part of broader settlement agreements are available at <https://oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp>.

4 The various compliance resource materials made available by the OIG can be found at <https://oig.hhs.gov/compliance/compliance-guidance/compliance-resource-material.asp>. The OIG also publishes educational materials, which are available at <https://oig.hhs.gov/compliance/101/index.asp>, for use by providers as part of their compliance programs.

5 The related portion of the current version of the Federal Sentencing Guidelines is available at [http://www.ussc.gov/Guidelines/2012\\_Guidelines/Manual\\_HTML/8b2\\_1.htm](http://www.ussc.gov/Guidelines/2012_Guidelines/Manual_HTML/8b2_1.htm).

purview. Recommended improvement should focus on how to better define the purpose and role of the compliance program from both an operational and strategic standpoint in supporting the entire organization.

With limited staff and resources, many compliance departments may not feel they are able to accomplish all the requirements of an ongoing and effective compliance program. However, there are other options that might be beneficial for facilities with limited staffing. Many vendors and consulting firms have tools and other resources that can assist in completing a review or the requirements necessary for an annual report on program compliance.

However, at the end of the day, it is the documentation that will corroborate results. Documentation of the compliance program's role within the organization is what will be requested by any of the agencies completing a review or an investigation.

### **Commitment**

The true difference between a “paper program” and an effective compliance plan is the demonstrated level of commitment on a daily basis to compliance throughout the organization. That commitment starts with the governing body in its compliance program oversight role, but requires bottom-up participation. All stakeholders of the organization, including board members, senior management, physicians, and all other employees participate in the elements that comprise the compliance program. As mentioned previously, it is imperative that documentation of training and education reports are maintained and readily available to any governmental agency or third party in order to demonstrate the commitment of the total organization to the program.

Compliance should be part of the organizational culture, as all employees should feel empowered to ask questions and report any concerns. As the OIG explains, providers “with an organizational culture that values compliance are more likely to have effective compliance programs and, thus, are better able to prevent, detect, and correct problems.”<sup>6</sup>

Having open lines of communication is as important as all other elements of the compliance program. An organization may be able to say it has an outstanding and well supported compliance program, but if the employees do not feel confident or comfortable enough to discuss a concern or violation they have witnessed, then the program has a significant weakness. Having open lines of communication with support for elements of the compliance program is important. Demonstrated actions of the board, physicians, executives, and management level directors are the true test of an organization's commitment to its compliance program.

To further gauge its compliance program's effectiveness, organizations should also conduct on-site interviews with directors, senior leadership, physicians, department managers, front-line managers, and staff, as appropriate. Depending on the

person's role within the organization, the interview questions should focus on the individual's familiarity with the compliance program, his/her willingness to participate in the compliance program (i.e., seek guidance, report concerns, cooperate with investigations), and his/her recommendations for improving the organization's compliance-related activities.

For an accurate assessment of an organization's culture (and opportunities for improvement), a reviewer should consider sending a questionnaire to a large number of employees using an electronic survey tool. Tools such as the Ethics Resource Center's (ERC) bi-annual National Business Ethics Survey® can serve as guides in developing such a questionnaire. ERC's survey includes, among other things, questions about observed misconduct, reporting of misconduct, perception of retaliation for reporting, and pressure to engage in misconduct.<sup>7</sup>

The end product of a compliance program audit should be a detailed, written report of the reviewer's findings and impressions, specific recommendations regarding the compliance program's structure and substance, and documented evidence of the organization's commitment to compliance. At a minimum, the report should include complete recommendations regarding: (1) the compliance program's structure, including specific roles and responsibilities from the governing body to front-line staff; (2) the scope of the compliance program and its relationship to other departments within the organization; (3) revisions to compliance program-related policies and procedures; and (4) ongoing education and promotion of the compliance program.

### **Post-Audit Action Plan**

In the hands of a dedicated compliance officer – one who regularly engages with all of the organization's constituencies – the compliance program audit report is an invaluable tool for directing resources to enhance the compliance program's effectiveness and efficiency. Working with other members of the management team, the compliance officer should develop an action plan for promptly addressing identified weaknesses. For example, if the report demonstrates a lack of understanding among employees regarding reporting mechanisms, the team should explore new, creative ways to promote this critical component of the compliance program.

In short, an effective compliance program is one to which all members of the organization share a strong commitment. The governing body and the management team share responsibility for setting expectations regarding the role of compliance in the organization. Interaction with the compliance program should not be a once-a-year education session or signature on a form. Instead, the compliance program should be continually re-evaluated and reinvented to remain relevant at all levels of organizational decision-making. ♦

6 OIG Supplemental Compliance Guidance for Hospitals, 70 Fed. Reg. 4858 (Jan, 31, 2005).

7 Information regarding the Ethics Resource Center and the survey is available at <http://www.ethics.org/nbes/findings.html>.





# CLINICAL COMPLIANCE EXPERTISE

## In the past few months, your client's risk potential for an audit has increased!

- More sophisticated fraud detection methods such as data mining
- New legislation has increased funding for audit programs
- All documentation is open to interpretation
- Government auditors can arrive with no advanced warning

### Partner with Simone to assist your clients in:

- Assessing current reimbursement, clinical & operational compliance
- Determining probe samples and statistically valid examples for disclosure
- Improving clinical documentation
- Reviewing the implementation of OIG 7 elements
- ZPIC and RAC audits
- Appealing denials

### Protect your clients:

▶ **CALL** 800.653.4043   **EMAIL** [info@simione.com](mailto:info@simione.com)   **VISIT** [simione.com](http://simione.com)

### Home care & hospice business solutions

**ORGANIZATIONAL**  
**FINANCIAL**  
**SALES & MARKETING**  
**TECHNOLOGY**  
**MERGERS & ACQUISITIONS**

**Simione**™  
HEALTHCARE CONSULTANTS

# Achieving Quality and Compliance in Home Health and Hospice Care

*Dolly M. Curley, Senior Manager, Simone Healthcare Consultants*  
*dcurley@simione.com*



## Introduction

If quality drives compliance, why is achieving both goals simultaneously such a difficult task for home health agencies (HHAs)? Could it be that providers of home health and hospice do not recognize the dual concepts of compliance and quality indicators? Have clinicians been focused on the laws and regulations under the Medicare payment system to the exclusion of quality indicators? Does the lack of focus and accountability on issues of compliance cause the industry to become less concerned about the laws and regulations and more about caring for their community at large, potentially leading us to losing sight of eligibility issues? All of these questions and the crucial connection between the delivery of quality care and meeting compliance requirements have recently become very relevant to both home health and hospice care providers.

## Home Health Care: The Need for Increased Attention to Compliance

For close to fifteen years, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) has promoted the voluntary adoption of compliance programs across the entire spectrum of healthcare providers. In 1998, it released its Compliance Program Guidance for Home Health Agencies.<sup>1</sup> In 2008, it published a revealing report finding repeated HHA deficiencies on three consecutive surveys, indicating that compliance was still not a priority.

The focus on compliance for home health agencies radically changed with the adoption of the Affordable Care Act (ACA), however. With the passage of this historic legislation, Congress

has for the first time mandated that a broad range of providers, suppliers, and physicians adopt a compliance and ethics program. The law now requires that as a condition of enrollment in federal healthcare payment programs, providers and suppliers must establish a compliance program that contains core elements to be established by HHS in consultation the OIG.<sup>2</sup> Because compliance with the Conditions of Participation (CoPs) is a prerequisite for payment, failure to implement a compliance program could lead to denial of claims and pose an audit risk.

Historically, if HHA's have not felt the need to develop a formal ethics and compliance program, the ACA provisions discussed above have definitely changed the landscape for these providers. The law creates a new opportunity for HHS and the OIG to adopt regulations that impose specific compliance standards intended to be "effective in preventing and detecting criminal, civil and administrative violations." Although the provisions in the ACA relating to compliance programs for skilled nursing facilities are quite detailed and contain an implementation timeline, the requirements for other providers and suppliers were not spelled out in the law. HHS is expected to release the core compliance elements for each industry sector on a rolling basis. However, given the low rate of compliance program implementation in the home health industry and CMS' increased focus on enrollment requirements for DME and home health, HHS may prioritize those sectors and release specific guidance for them first.

The OIG's FY 2013 Work Plan offers some clues on forthcoming potential areas of focus for home health compliance requirements, which HHAs may want to consider. For example, the Work Plan lists the following enforcement targets:

<sup>1</sup> 63 Fed. Reg. 42,410.

<sup>2</sup> See Sections 6102 and 6401 of the Affordable Care Act.

- » Compliance with home health face-to-face requirements, which stipulate that physicians who certify beneficiaries as eligible for Medicare home health services have face-to-face encounters with the beneficiaries;
- » Compliance with state requirements that criminal background checks be conducted for HHA applicants and employees;
- » The timeliness of HHA recertification and complaint surveys by state survey agencies and accreditations organizations. OIG will also look at CMS oversight in this area, which is designed to monitor HHA surveys and thereby ensure HHA compliance with Medicare CoPs;
- » Missing or incorrect patient outcome and assessment data in the Outcome and Assessment Information Set (OASIS) data to identify payments for episodes for which OASIS data was not submitted or for which the billing codes on the claims are inconsistent with OASIS date;
- » CMS's and Medicare Administrative Contractors oversight activities performed to identify and prevent improper home health payments from January to October 2011;
- » Compliance with home health Prospective Payment System Requirements (PPS) including the documentation required in support of the claims paid by Medicare;

For those organizations that have not initiated a compliance program in their agency, it is critical for them to do so now. While waiting for HHS to roll out compliance standards for HHAs, the OIG's Compliance Program Guidance can be a valuable tool in helping home health agencies begin that process. The Guidance identifies seven elements that should be included in every compliance and ethical Program and are based on criteria adopted by the Federal Government in the Federal Sentencing Guidelines. The seven elements include:

- » Developing and distributing written standards of conduct, policies, and procedures that reflect the institution's commitment to a compliance Code Of Conduct
- » Designating a Compliance Officer and Committee
- » Conducting "effective" training and education
- » Develop "effective" open Lines of Communication
- » Internal auditing and monitoring
- » Enforcing standards through well-publicized disciplinary guidelines

- » Responding to detected offenses and developing a plan of correction

The seven elements listed above and the targeted areas of enforcement in the OIG Work Plan are an excellent guide for beginning the process of establishing a formal HHA compliance program. While developing and implementing a compliance plan does not protect an HHA from liability under federal fraud and abuse laws, a facility that makes a reasonable effort to follow a compliance plan may earn some degree of leniency from the OIG if it discovers any deficiencies or violations.

CMS has already implemented increased oversight by auditors and a range of alternative sanctions against HHAs found to have deficiencies that constitute noncompliance with Medicare Conditions of Participation. On November 8, 2012, CMS finalized a regulation that allows it to impose intermediate sanctions when it has concerns about an HHA's conduct.<sup>3</sup> Starting in July 2014, CMS can impose fines of \$500 to \$10,000 per day depending on the severity of the violation. CMS also has the authority to mandate plans of correction, temporary management, and in service training. The rule also revises the existing Conditions of Participation (CoPs) that home health agencies must meet to participate in the Medicare program. The CoPs were last revised in 1989. According to CMS, the new requirements will focus on the actual care delivered to patients by HHAs, reflect an interdisciplinary view of patient care, allow HHAs greater flexibility in meeting quality standards, and eliminate unnecessary procedural requirements.

Figure 1 on page 57 illustrates the sanctions that went into effect July 2013.

Under this new set of rules, home health agencies need to pay greater attention to compliance efforts and take measures to prevent a citation. First, HHAs must be aware that the Plan of Care (POC) issues continue to be the focus in CMS survey deficiencies. HHA's have expertise in this area, as the POC reflects the physician's orders which the nurse and other clinicians are expected to follow. Communication with the physician is evidenced through documentation. The creation of new processes for increasing physician communication and collaboration with the clinical staff, and making sure that documentation reflects that interaction would be an excellent way to tighten the reins around the POC.

## Hospice Care and Compliance Concerns

Hospice care, utilizing a holistic approach, was developed in response to the needs of patients who are in their final stages of life, and provides the right and the privilege of dying at home with dignity. In 1982, the Medicare Hospice Benefit was established under the Tax Equity and Fiscal Responsibility Act (TEFRA). Over the past few decades, questionable certifications and re-certifications of terminal illness led to the Hospice Interpretive Guidelines mirroring hospice requirements in Medicare

3 Fed. Reg. 67068, November 8, 2012.

Figure 1

Final Rule Survey Changes	
Sanctions	Details
Temporary management	CMS appoints a temporary manager whose salary the agency must pay. The temporary manager has authority to hire, fire, and reassign staff.
Suspension of payment	Agencies will not receive payment for any new admissions that start on or after the sanction effective date. The agency may not charge new patients for services unless it can demonstrate that patients caregivers were informed orally and in writing that Medicare may not cover services.
Civil money penalties	Penalties cannot exceed \$10,000 and can be imposed on a per-day or per-instance basis. Per-day penalties begin on the day a surveyor identifies the deficiency. Per-Instance penalties are imposed for specific instances of non-compliance that were resolved during the survey.
Directed plan of correction	CMS or a temporary manager appointed by CMS creates a targeted plan of correction to remedy specific deficiencies.
Directed in-service training	The agency must pay for in-service trainings by established learning institutions.

CoPs. According to Medpac, questionable practices involved unusually high rates of live discharges, increases in length of stay (LOS) over 180 days and a fragmented fee-for-service system.<sup>4</sup>

To qualify for hospice care, beneficiaries must be eligible for Medicare Part A, have a terminal illness with a prognosis of 6 months or less that is certified by a physician, assuming the illness runs its normal course, must receive treatment from a Medicare-approved hospice and sign away their right to curative treatment for the terminal conditions. A physician must certify the medical necessity of the initial ninety-day period of hospice care. With passage of the Affordable Care Act in March 2010, Congress required hospice physicians or hospice nurse practitioners to have a face-to-face encounter with Medicare hospice patients prior to the 180th-day recertification and every recertification thereafter, and to attest that the encounter occurred. Hospice certifications and re-certifications must include a brief narrative from the physician identifying the clinical findings that support a life expectancy of six months or less. It also mandates that for a patient requiring a third or later benefit period, the physician must explain why the clinical findings of the face-to-face encounter support a life expectancy of six months or less.

Hospice care is also targeted for an uptick in scrutiny by government enforcement agencies. Again looking at OIG Work Plan for 2013, hospice providers need to ramp up compliance efforts in the following areas:

- » Marketing practices and financial relationships with nursing facilities
- » Acute care hospital inpatient transfers to inpatient hospice care
- » Inappropriate enrollment compensation

» Medicaid payments and compliance with Federal reimbursement requirements

» Duplicate drug claims under part D and under Part A

While Hospice is a distinct specialty that provides the dying and their families' exceptional physical, psychosocial, and spiritual care, providers cannot lose sight of their accountability in compliance, quality of care, and reimbursement. Training and education in these areas will better prepare your agency for a successful audit.

- A. The documentation is key to showing evidence of eligibility. The clinicians and physicians must show evidence of an 'event' or significant change as a reason for re-certification. Missing vital information such as monthly weights and measurements and/or pre-admission paperwork; vague statements week after week, month after month such as 'weaker' or 'sleeping more,' custodial and/or chronic care do not meet eligibility.
- B. Make sure your forms meet CMS requirements

### Does Quality = Compliance?

Now that we have established a baseline for developing a compliance program, how do we define quality? Can quality be measured objectively and identified by an administrator, a clinician or a patient? By whose standard do we follow? How does the definition of quality differ between stakeholders? Indicators need to be very specific in order to actually validate appropriate outcomes. Outcomes for quality measures must be clearly supported by the clinical documentation, providing evidence of the assessment of the patient, the interventions provided, and the delivery of care by all disciplines. The written word can provide misleading clinical information if not accurate. For example, the

4 Medpac, June 2013 Report of Congress, [www.nahc.org/NAHCRReport/nr130529\\_2](http://www.nahc.org/NAHCRReport/nr130529_2).



fundamental purpose of a completed OASIS on admission is for the evaluation of Medicare eligibility for admission to home care. If inaccurate, the diagnosis and plan of care will be skewed and the outcomes at discharge not valid. Therefore, it is the responsibility of the agency to provide on-going training and education for continuous performance improvement.

A patient may identify and measure what constitutes quality completely different from what is actually being measured by the clinician and HHA. It is necessary to consider that a patient may perceive that his home care was excellent simply because the same clinician provided the majority of his care. Satisfaction surveys may indicate the patient's belief that his care was good simply based on the notion that continuity of care by the same clinician infers quality of care. Alternatively, a nurse measuring quality is likely to use other measures, such as assessing the patient's improvement, taking responsibility, and ownership of the disease process, managing medications and preventing re-hospitalization. Indicators of quality that are measured by outcomes are not necessarily what the patient views as quality but reflect standards by which clinicians practice. Both measurements are valid, and the key is true statement that quality is in the eye of the beholder. Compliance means that a facility operates in accordance with established guidelines and legislation and may not be of concern to the patient. It is more likely that healthcare professionals will see the relationship between quality and compliance as more of a mirror image of one another and believe that quality does in fact drive compliance.

### Strategies for Achieving Quality Improvement and a Successful Compliance Program

Delivering quality care today and in the future will require both communication and collaboration interdepartmentally. Being knowledgeable in how your role and responsibilities impact on another department is essential to the breakdown of silos and bringing accountability to all. Home care agencies are busy scrutinizing computer systems and programs that can drive compliance and prompt non-compliance but it is in optimizing your homecare resources that will deliver outcome-driven care. For instance, effective billing should involve a process that brings together the OASIS and coding specialists, performance improvement and education departments along with home care staff to drive a compliant team. Initiating an ongoing compliance audit whereby regulations, evidence-based practices, and care coordination can be shared and discussed amongst the team prior to submission of bills can be invaluable in preventing red flags and financial risk while increasing clinical and regulatory knowledge.

The delivery of quality of care and maintaining a supportive role in patient advocacy has and always will be essential to our practice. However, clinicians now have an accountability to advance their expertise in the areas of reimbursement and regulatory demands. Making decisions in home health can be

about acceptance of referral to number of visits to re-certification, which requires not only a strong clinical background but also an understanding of CMS eligibility. Documentation must support this eligibility for reimbursement. HHAs who promote education will ultimately drive compliance, improve reputation, and lead to better patient outcomes. Home Health certification may be just the answer in the near future to ensure expertise in this specialty field.

### Checklist for Home Health and Hospice Compliance

- » Develop a code of conduct and effective compliance program.
- » Follow the 7 Elements of the OIG Model Compliance Program and pay special attention to the OIG's Annual Work Plan.
- » Motivate and encourage staff involvement.
- » Provide CoP training in areas of *Homebound Status*, *Medical Necessity* and *Laws of Compliance* at every orientation and as an annual review with testing.
- » Improve relationships and communication between staff and physicians.
- » Develop and Train a Rapid response Team (RRT) for ADR's, RAC's, and ZPIC requests and utilize external assistance to review prior to submission.

Audit your HHA's HIPAA compliance.

- » Evaluate your compliance plan as an on-going process within the organization's regular operations, and share findings with staff.
- » Conduct compliance audits of probe samples under attorney/client privilege in order to identify potential risk areas and develop action plans to address identified risks.
- » Evaluate external audit results and develop a response strategy to address and appeal if necessary audit findings.
- » Correlate the diagnosis codes to the written and signed POC and documented interventions, individualizing POCs for every patient instead of using the same "one stop shopping plan" for everyone.
- » Provide effective documentation education. Monitor compliance with documentation policies regularly to ensure compliance and amend processes as soon as needed.



## References

1. *The Survey Requirements and Alternative Sanctions for Home Health Agencies 1991*. OIG. [hhs.gov/oei/reports/oei-06-11-00401](http://hhs.gov/oei/reports/oei-06-11-00401), March 2, 2012.
2. HHS OIG Work Plan FY 2012. Department of Health & Human Services (HHS), OIG *Work Plan*, Fiscal Year 2012. website <http://org.hhs.gov/reports-and-publications/archivesworkplan/2012/Work-Plan-2012.pdf>. Accessed June, 2013.
3. The Seven Elements of an Effective Compliance Program. Available online at [www.healthcentercompliance.com/seven-elements](http://www.healthcentercompliance.com/seven-elements). Accessed July 2013.
4. Friedman, B. and Basu J. *The Rate and Cost of Hospital Readmissions for Preventable Conditions*. Med. Care Res Rev June (2004). Vol. 61: 225-240.
5. Bensatt, J. and Taragin, M. (2000). Hospital Readmissions as a Measure of Quality. *Archives of Internal Medicine* 160 (April): 1074-81.
6. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. website <http://www.hhs.gov/ocr/privacy>. Accessed June 2013.
7. Marx, D. (2010). *The Just Culture Algorithm*. Outcome Engineering, LLC. Just What Does Culture have to do with Patient Safety? Available online at [www.medscape.com/viewarticle/71467](http://www.medscape.com/viewarticle/71467).
8. Leaps, L. (January 25, 2000). Testimony, United States Congress, United States Senate Subcommittee on Labor Health and Human Services and Education. [www.hhs.gov/asl/testify/2008/testimony.html](http://www.hhs.gov/asl/testify/2008/testimony.html). Accessed June 2013.
9. ANA Position Statement. (January 28, 2010) *Just Culture Concept*. website. [www.http://nursingworld.org/psjustculture](http://www.nursingworld.org/psjustculture). Accessed June 2013.
10. Medpac June Report to Congress June 2013. [www.nahc.org/NAHC-Report/nr130529\\_2/](http://www.nahc.org/NAHC-Report/nr130529_2/) Accessed July 2013.

# AHLA

## Check Out this Fraud and Compliance Title from AHLA!



*Medicare Law, 3rd Edition* leads readers through the maze that is the Medicare program. Fraud and abuse issues have become increasingly intertwined with broader Medicare regulatory issues, from billing issues resulting in false claims actions to the growing use of Medicare enrollment revocation to address fraud and abuse concerns. This new edition of *Medicare Law* provides up-to-date guidance fraud and abuse practitioners need.

For more information or to order, please visit [www.healthlawyers.org/bookstore](http://www.healthlawyers.org/bookstore) or call 800-533-1637.





**At the forefront  
of compliance...**

**for over 20 years.**

For more than 20 years and over 3,000 companies, Strategic Management (SM) has been an **industry leader in advancing health care compliance and regulatory strategies** for many of the nation's most sophisticated and prestigious health care organizations. Founded by Richard Kusserow, former HHS Inspector General, SM was the first health care consulting firm to focus on compliance programs. SM consultants are among the most experienced in the industry offering in depth experience working in both government and private sector health care arenas. SM remains at the **forefront of compliance with regulatory and enforcement requirements, as well as business best practices.**

Strategic Management services include:

- |  |                                     |
|--|-------------------------------------|
| ✓ Compliance Program Effectiveness Evaluations | ✓ Physician Arrangements Reviews    |
| ✓ Claims Data Analysis                         | ✓ Responding to Government Auditors |
| ✓ HIPAA and HITECH Act Compliance              | ✓ Regulatory Analysis               |
| ✓ Independent Review Organization              | ✓ Risk Assessment and Management    |
| ✓ Interim Compliance Officers                  | ✓ Internal Investigation Services   |
| ✓ Litigation Support                           | ✓ Compliance Resource Center        |

**Stay current with the regulatory/enforcement environment  
with Richard Kusserow's blog:**

<http://healthcarecompliance.wordpress.com>

Visit us at [www.compliance.com](http://www.compliance.com), 703.683.9600 or email us at [compliance@strategicm.com](mailto:compliance@strategicm.com) to discuss solutions.

# Challenging Overpayment Extrapolations: Statistical Considerations

*Cornelia M. Dorfschmid, Ph.D., Executive Vice President  
Strategic Management Services, LLC, [cdorfschmid@strategicm.com](mailto:cdorfschmid@strategicm.com)*



## Contractor Reform and HEAT

### HEAT

The government has recovered a record-breaking \$10.7 billion in recoveries of health care fraud in the last three years, and contractor reform and new initiatives have contributed to that success. In 2009, the Department of Health and Human Services (HHS) and Department of Justice (DOJ) created the Health Care Fraud Prevention and Enforcement Action Team (HEAT).<sup>1</sup> With its creation, the fight against Medicare fraud became a Cabinet-level priority. HEAT's work is directed by the Secretary of HHS and the Attorney General. The Centers for Medicare & Medicaid Services (CMS) are also strongly committed to combating provider fraud, waste, and abuse through nationally coordinated strategies and new contractors focused on claims audit, investigation, and recovery. In recent years, both states and CMS at the national level have increased their focus on coordinating fraud enforcement efforts. The Medicare Integrity Program was established by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and later, the Medicaid Integrity Program was established by the Deficit Reduction Act (DRA) of 2005. These efforts, along with administrative contractor consolidation and implementation of new recovery contractors, led to record recoveries. Among other things, the high rate of recovery is due to the use of statistical overpayment extrapolation to assess damages.

### Medicare

The Medicare Prescription Drug, Improvement, and Modernization Act (MMA) of 2003 brought consolidation of the Fiscal Intermediaries and Carriers. They were consolidated into the new Medicare Administrative Contractors (MACs), which are now processing both Part A and B claims. Contractor reform under the MMA also brought further consolidation with the seven Zone Program Integrity Contractors (ZPICs), which took over the role of the Program Safeguard Contractors (PSCs) and are fraud-focused. Furthermore, MMA established the Medicare Recovery Audit Contractors (RACs), which work directly for CMS and are paid on a contingency basis. The RAC program was made permanent after a successful Demonstration program. Four Medicare RACs are now fully operational in all states and actively auditing claims.<sup>2</sup> These Medicare contractors are allowed to extrapolate overpayments that they identify, and have made this a part of their activities

### Medicaid

The Medicaid Integrity Program (MIP) is the first comprehensive federal strategy designed to prevent and reduce provider fraud, waste, and abuse in the \$300 billion per year Medicaid program. It is outlined in the Comprehensive Medicaid Integrity Plan (CMIP) and managed centrally by the Medicaid Integrity Group (MIG) within the Center for Medicaid and State Operations (CMSO) at CMS. The Medicaid Integrity Contractors (MICs) include Review, Education, and Audit MICs. Audit MICs

<sup>1</sup> See, HEAT Task Force <http://www.stopmedicarefraud.gov/aboutfraud/heattaskforce/>.

<sup>2</sup> See, the Recovery Audit Program webpage at [www.cms.gov](http://www.cms.gov).



audit claims and are not paid on a contingency basis but are compensated differently. Although they do not participate in the recovery of the overpayments they identify, their responsibilities still involve discovering and recovering overpayments. Note that when HHS OIG audited the Audit MICs' performance, it found that their performance was hindered due to poor data and target identification.<sup>3</sup> The MIG used sampling and extrapolation during test audits and plans to systematically pursue greater use of extrapolation in the future, when the data are refined and a gold standard MIG sampling plan is developed.<sup>4</sup>

The Affordable Care Act (ACA) also expanded the Recovery Audit Contractor program from Medicare to Medicaid and requires each state Medicaid program to establish a Medicaid RAC program, absent an exception, to enable the auditing of claims for services furnished by Medicaid providers. These Medicaid RACs are also paid on a contingency basis, work directly for the state and must identify overpayments and underpayments. States and their Medicaid RACs must coordinate their recovery audit efforts with various other contractors or entities that perform audits of entities receiving Medicaid payments, including DOJ, the Federal Bureau of Investigation (FBI), the Office Inspector General of the Department of Health and Human Services (HHS OIG), and the State Medicaid Fraud Control Units (MFCU).<sup>5,6,7</sup> Lastly, HHS OIG and MFCUs initiate or conduct their own investigations and audits, and may use extrapolated overpayments from sample findings.

### Overpayment Extrapolation is Here to Stay

Contractors, such as the ZPICs, RACs, and MICs are allowed by their task order with the government to data mine and extrapolate. They typically aim to identify inappropriate payment amounts that are relatively large by analyzing large sets of claims and detecting systemic errors using "automated review," i.e., computerized analysis that does not require medical review. Alternatively, they use a type of "complex review" that requires sampling, for which they request and analyze medical charts and billing records for a sample of claims. Allegedly inappropriate payments can then be extrapolated from a sample to a large universe of claims. The samples can be as few as thirty claims, regardless of the size of the universe,<sup>8</sup> but even the relatively small samples can lead to huge recovery demands in the thousands and millions of dollars.

When individuals and entities are faced with a recovery demand involving overpayment extrapolation from any of these contractors, the medical, clinical and coverage criteria must all be considered for a successful challenge. Equally important in challenging the demand are the statistical calculations that affect whether an extrapolation is valid and justified. Statistical audit results should hold up to scrutiny by statistical experts and under generally acceptable auditing standards.

Some proactive providers and suppliers have become much more sophisticated in analyzing and mining their own claims to detect unusual patterns or high risk profiles to avoid becoming an audit target and avoiding overpayment extrapolations altogether. Regardless of these precautions, providers and suppliers should expect to eventually face a government audit, and should therefore implement risk mitigation strategies. A health care organization's risk control strategy should therefore include preparing for a government audit. Providers need to be aware of the basics of statistical sampling and claims auditing techniques in order to best assess and, as appropriate, challenge the government auditors' overpayment extrapolations.

### Requirements for Extrapolation - Legal and Other Considerations

There are limitations on when statistical sampling before extrapolation can occur and when recovery of refunds can be based on extrapolation. Statistical sampling can be used to calculate and project (i.e., extrapolate) the amount of overpayment(s) made on claims, but only when certain pre-conditions are met, such as those defined for Medicare contractors. MMA Section 935 puts limitations on the use of extrapolation.<sup>9,10</sup> Consistent with Section 935 of the MMA, the CMS Medicare Integrity Program Manual (PIM) provides instructions for PSCs, ZPIC Business Integrity (BI) units, and contractor Medical Review (MR) units on the use of statistical sampling and when they can extrapolate. According to the PIM, MMA mandates that before using extrapolation to determine overpayment amounts, there must be a determination of (1) sustained or high level of payment error, or, 2) documentation that educational intervention has failed to correct the payment error. However, while extrapolation may be used if either of these two conditions is present, the determination that a sustained or high level of payment error exists is not

3 HHS OIG, Medicaid Integrity Program Report for Fiscal Year 2012; [http://oig.hhs.gov/reports-and-publications/medicaid-integrity/2012/medicaid\\_integrity\\_reportFY12.pdf](http://oig.hhs.gov/reports-and-publications/medicaid-integrity/2012/medicaid_integrity_reportFY12.pdf).

4 See, Medicaid Program Integrity Manual-Ch. 9-Data Analysis, 9010 – SAMPLING AND EXTRAPOLATION (Rev. 1, Issued: 09-23-11, Effective: 09-23-11, Implementation: 09-23-11). <http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mpi115c09.pdf>.

5 See, HEAT Task Force <http://www.stopmedicarefraud.gov/aboutfraud/heattaskforce/>.

6 Frequently Asked Questions Section 6411(a) of the Affordable Care Act December 2011 [http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/MedicaidIntegrityProgram/Downloads/Medicaid\\_RAC\\_FAQ.pdf](http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/MedicaidIntegrityProgram/Downloads/Medicaid_RAC_FAQ.pdf).

7 Cornelia M. Dorfschmid, Medicaid Integrity Contractor Reform: MAC, MIC, ZPIC, RAC, *Compliance Today* (Jan 2010).

8 See, Rachel H. Park & Lester J. Perling, Statistical Sampling: Evolving Legal Issues, AHLA white paper [http://www.healthlawyers.org/Events/Programs/Materials/Documents/MM12/papers/D\\_park\\_perling.pdf](http://www.healthlawyers.org/Events/Programs/Materials/Documents/MM12/papers/D_park_perling.pdf).

9 See, CMS, MLN Matters (MM6183 Revised), Limitation on Recoupment (935) for Provider, Physicians and Suppliers Overpayments. <http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/MM6183.pdf>.

10 See, Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Section 935. RECOVERY OF OVERPAYMENTS. <http://www.gpo.gov/fdsys/pkg/PLAW-108publ173/pdf/PLAW-108publ173.pdf>.

subject to administrative or judicial review.<sup>11</sup> Still, the steps must have been taken by the contractor.

There are also general guidelines that must be followed by government auditors and that may be considered when challenging overpayment assessments. The Government Auditing Standards (the “Yellow Book”) contains standards for audits of government organizations, programs, activities, and functions, and for audits of government assistance received by contractors, nonprofit organizations, and other nongovernment organizations. These standards, often referred to as Generally Accepted Government Auditing Standards (GAGAS), are to be followed by auditors and audit organizations when required by law, regulation, contract, or policy. The standards govern the auditors’ professional qualifications, the quality of the audit effort, and the characteristics of professional and meaningful audit reports.<sup>12</sup>

Objectivity and independence are the key aspects of GAGAS. Adherence to clear criteria based on applicable and well documented standards and processes that conform to inter-rater reliability in auditing are critical to maintaining objectivity and defensibility of the audit findings. Inter-rater reliability is an especially important feature in statistical audit results involving findings of overpayment. These findings should be prepared in a manner that allows for validation and verification of assumptions, methods, and results, including verification through replication of results, in a dispute or challenge.

Furthermore a government auditor’s statistical analysis can be challenged on technical grounds. For example, the PIM sets forth the most detailed guidelines to be followed by Medicare contractors in performing statistical sampling. If the Medicare contractor fails to follow these guidelines, the extrapolation is subject to challenge and reversal upon appeal. In comparison, guidance for Medicaid contractors and state agencies conducting audits using overpayment extrapolation is less detailed and consistent. Accordingly, as part of an audit defense, it is important to obtain the guidance and if possible audit manuals that Medicaid contractors must follow in a particular state to ensure the contractor followed these guidelines.

HHS OIG also provided some guidance on extrapolation in its original OIG’s Provider Self-Disclosure Protocol (SDP) of 1998 and then again in the updates to its Protocol in 2013. Statistical concepts such as sample size or precision/confidence levels and type of estimation are referenced in the Protocol and may serve as evidence of a ‘best practice’ in defending against allegations of overpayments based on extrapolations.<sup>13</sup>

## A Well Organized Response

When responding to a demand letter, recovery amount determination, or damage assessment that is based on sampling and overpayment extrapolation, providers and their attorneys must

develop a technical response that includes, as necessary:

- » Statistical expertise in sampling and statistical formula, OIG RAT-STATS (a statistical package recommended by and available from the HHS OIG website), Statistical Analysis System (SAS),<sup>14</sup> R software,<sup>15</sup> SPSS, and other statistical applications used by auditors;
- » Clinical and Health Information Management (HIM) expertise to assess medical necessity, clinical standards, and coding and billing accuracy; and
- » Regulatory and legal expertise to assess coverage criteria, payer rules, and applicable federal and state law.

While many government auditors rely on the use of RAT-STATS or SAS for sampling and estimation, not all do. State agencies may use even customized software or other packages, while others use MS Excel, or a mix of manual calculation and software packages. Whatever method a government auditor uses to get to the extrapolation, it must still follow the rules of a “fair” game using sampling. Not just any sampling will do; one must utilize a statistically valid random sample (SVRS), which is inherently fair and replicable. SVRS is also the only type of sampling that can generate a representative sample that is objective and replicable. A recovery request must be based on a fair and professionally documented process that allows for verification by an independent and knowledgeable party. Inter-rater reliability should be assured through proper audit work papers and documentation of the audit.

## Statistical Documentation Matters

A demand letter from a government contractor requesting repayment of claims that were allegedly paid inappropriately usually states the audit objective and reasons for the audit, the estimated amount, confidence levels, methods, randomization, characteristics measured, and findings. In other situations, such as fraud investigations or *qui tam* suits, the documentation relating to the statistical concepts and aspects of the damage assessment proposed for settlement may be less readily available and obvious. In that case, a detailed document request to the government agency for the documentation that explains the statistical foundation of the estimate along with a meticulous analysis by the audit target, including the development of the provider’s own estimate for counterproposals, becomes necessary. A statistical review to fully understand how the government auditor or agency arrived at its estimates is most important when damage assessments are the basis on which fines and multipliers are calculated.

When providers face a recovery demand, their staff and the provider’s inside and/or outside counsel often first focus on a defense strategy that challenges the findings from a medical

11 See Medicare Program Integrity Manual, Chapter 8, Section 8.4.1.2 <http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/pim83c08.pdf>.

12 See, 2011 Internet Version of Government Auditing Standards (August 2011) <http://www.gao.gov/yellowbook>.

13 See, HHS OIG website at Self Disclosure Information <http://oig.hhs.gov/compliance/self-disclosure-info/index.aspx>.

14 SAS is a commercial and renowned statistical package. See [www.sas.com](http://www.sas.com).

15 R is a free statistical package. See, [www.r-project.org](http://www.r-project.org).



review point, looking for arguments and information to address why the individual claims complied with coverage criteria and medical necessity. Obviously this is vital, as each claim that can be overturned and deemed error free can be expanded to the universe of all related claims. However, one also needs to keep in mind that whenever sampling is the basis for the estimate, the audit target (the provider) should be afforded the opportunity to verify the validity of the sampling and sampling methods. One would expect that an objective and independent audit consistent with GAGAS standards would be documented to allow for such verification and validation.

For an overpayment extrapolation to pass scrutiny, it is critical that the underlying sample be statistically valid and support a representative and objective estimate. All too often, this aspect of verification is set aside in the early phases of elaborating a defense strategy, and the immediate focus becomes re-analyzing the claims for medical necessity or compliance with other coverage and documentation requirements. This may simply be due to the fact that the statistics aspects of the audit are outside the provider's or attorney's expertise. Expense and resource constraints may be another reason. However, ignoring potential statistical challenges to the assessment may be a strategic mistake because if a sample is not statistically valid, any projection is invalid. Furthermore, even if the sample is proven valid, the estimation itself may be flawed.

With this mind, a solid response to a government contractor or agency's demand requesting recovery of extrapolated overpayments can be separated into a three-pronged approach:<sup>16</sup>

- » Assess the statistical validity of the sampling in the audit. Assess the validity of the random sampling method as it relates to the estimation technique.
- » Assess the validity of the sample actually drawn.
- » Assess the criteria and characteristics applied in the sample against clinical and documentation requirements for compliance with coverage rules of the audit.
- » If the sample is valid, assess the overpayment estimate to evaluate the estimation technique and accuracy of the execution of the extrapolation, including confidence and precision levels. Re-estimate and generate a counter-estimate of overpayment, if the sample is drawn in a statistically valid manner but there is disagreement on the clinical and regulatory criteria applied to the individual claims in the auditor's sample. Consider reviewing your own sample if the auditor's sample is invalid.

## Things To Consider When Faced with Overpayment Extrapolation

**In conclusion the following considerations may facilitate a review or challenge of an overpayment extrapolation.**

1. Government auditors can make errors. Do not assume the statistical portion of the audit is necessarily correct.
2. Engage legal counsel and statistical expertise early rather than late in the appeals process for an effective defense strategy.
3. Know the legal and statistical requirements imposed on the particular contractor or agency by statute and in the various manuals such as the PIM in Medicare, state agency audit manuals, etc.
4. Request the sampling plan, universe, and sample frame regardless of what was provided with the auditor's report of findings.
5. Request the random numbers and information on the random number generator used.
6. Check for a probability sample and ensure that the sampling can be replicated. Judgmental samples do not allow for objective and valid extrapolation.
7. Verify that the sampling method is consistent with the method of appraisal.
8. Verify the statistical validity of the sample. Regenerate the sample.
9. Ensure the audit universe is properly assembled and consistent with the sample frame.
10. Verify that the estimate is reported as required by the federal or state agency, e.g., such as in Medicare in accordance with the PIM.
11. Ensure confidence levels are reported and assess whether the lower limit is the basis of the recovery amount. If not, consider aiming for this as a ceiling in any settlement negotiations rather than the Point Estimate, especially when statistical precision is low.
12. If the sample is invalid, self-assess with a probe to get a sense of what the underlying claims overpayment risk really is. Be prepared to refund what you identify with error.
13. Reanalyze the data claim-by-claim, using an independent auditor with appropriate credentials and credibility. If the overpayment in a claim-by-claim analysis refutes the government auditor's sample results, re-estimate and engage a statistical expert using RAT-STATS or similar packages and the appropriate statistical formula.

<sup>16</sup> See also, Cornelia Dorfschmid, OIG RAT-STATS: Response Strategies to Government Claims Audits, *Compliance Today*, Vol. 12, April 2010.

**Compliance is never 100% perfect.  
What happens if something goes wrong?  
A few simple words can make a big difference.**

“Any dispute arising out of or relating to this contract or the subject matter thereof, or any breach of this contract, including any dispute regarding the scope of this clause, will be resolved through arbitration administered by the American Health Lawyers Association Dispute Resolution Service and conducted pursuant to the AHLA Rules of Procedure for Arbitration. Judgment on the award may be entered and enforced in any court having jurisdiction.”



**Always Have a Backup Plan**

**Include the AHLA Dispute Resolution Service in all the contracts you draft.  
Your clients will appreciate it.**

**For more information visit our website at [www.healthlawyers.org/DRS](http://www.healthlawyers.org/DRS)**

## Upcoming Programs



### **Fraud and Compliance Forum**

September 29-October 1, 2013,  
Hilton Hotel, Baltimore, MD, *Co-sponsored with the Health Care Compliance Association (HCCA) HealthCare Appraisers, Inc. and Deloitte Financial Advisory Services, LLP have provided sponsorship in support of this program.*



### **Long Term Care and the Law**

February 19-20, 2014, The Cosmopolitan of Las Vegas Hotel, Las Vegas, NV  
*Plante Moran PLLC and Principle Valuation LLC have provided sponsorship in support of this program.*



### **Tax Issues for Healthcare Organizations**

October 20-22, 2013, Ritz-Carlton Pentagon City, Arlington, VA  
*PYA has provided sponsorship in support of this program.*



### **Institute on Medicare and Medicaid Payment Issues**

March 26-28, 2014, Baltimore Waterfront Marriott Hotel, Baltimore, MD



### **Fundamentals of Health Law**

November 3-5, 2013. Chicago Marriott Magnificent Mile, Chicago, IL



### **Healthcare Transactions**

April 10-11, 2014, Loews Vanderbilt Hotel Nashville, Nashville, TN



### **Legal Issues Affecting Academic Medical Centers and Other Teaching Institutions**

January 23-24, 2014, Ritz-Carlton Hotel, Washington, DC



### **Antitrust in Healthcare**

May 13-14, 2014, Arlington, VA  
*Co-sponsored with the American Bar Association's Health Law Section and Section of Antitrust Law*



### **Physicians and Hospitals Law Institute**

February 5-7, 2014, Sheraton New Orleans, New Orleans, LA  
*Platinum Sponsor: HORNE LLP*



### **In-House Counsel Program and Annual Meeting**

June 29-July 2, 2014, New York Hilton Hotel, New York, NY

**For more information on all our upcoming programs,  
go to [www.healthlawyers.org/programs](http://www.healthlawyers.org/programs)**