

COMPLIANCE TODAY

MAGAZINE

JANUARY 2019



Workplace violence:
What compliance professionals
should know about
the unthinkable (P18)

**Controlling mobile devices in
an academic medical center:**
Unique challenges (P22)

**Compliance tips for implementing
an electronic medical
record system (P28)**

Tried and true survey readiness
(P34)

GREG RADINSKY

SENIOR VICE PRESIDENT &
CHIEF CORPORATE COMPLIANCE OFFICER
NORTHWELL HEALTH

SEEING ENFORCEMENT ISSUES FROM ALL SIDES

(P12)



HCCATM



Articles

42 **Got privilege? Best practices to protect privileges during an internal investigation**

by **James Holloway**

Attorney-client privilege and work product privilege must be carefully established, guarded, and used appropriately to protect incriminating evidence from discovery.

46 **Payment collection controls**

by **Darryl Rhames**

Standardizing the collections process, training cashiers, and protecting the assets from fraud and theft can all have a positive effect on your revenue cycle.

52 **[CEU] New CMS rule revisions affecting your inpatient rehabilitation facility**

by **Danielle C. Gordet**

A look at the FY 2019 revisions to the IRF final rule regarding coverage requirements and recommendations to help you ensure compliance at your facility.

56 **[CEU] Physician compensation arrangements: Robust reviews are a must**

by **Tynan O. Kugler and Susan Thomas**

A solid compensation review process, including a helpful checklist, to help ensure that contracts are negotiated and maintained in compliance with regulatory guidelines.

64 **How to build a positive relationship with your CIA independent monitor**

by **J. Veronica Xu**

For long-term care providers, a court-appointed monitor can be a helpful partner and resource if you understand their role and responsibilities, and work with them rather than against them.

68 **Print and ePresentation: New rules for managed care organizations**

by **Deb Mabari and Doug Pray**

Medicare Advantage and Part D plan sponsors can now distribute specific types of plan benefit information electronically, saving time and money.

EDITORIAL BOARD

Gabriel Imperato, Esq., CHC, CT Contributing Editor
Managing Partner, Broad and Cassel

Donna Abbondandolo, CHC, CHPC, CPHQ, RHIA, CCS, CPC
Sr. Director, Compliance, Westchester Medical Center

Nancy J. Beckley, MS, MBA, CHC,
President, Nancy Beckley & Associates LLC

Robert Carpino, JD, CHC, CISA
Chief Compliance and Privacy Officer, Avanti Hospitals, LLC

Charles E. Colitre, BBA, CHC, CHPC, Compliance and
Privacy Officer, Crystal Clinic Orthopaedic Center

Cornelia Dorfschmid, PhD, MSIS, PMP, CHC
Executive Vice President, Strategic Management Services, LLC

Tom Ealey, Professor of Business Administration, Alma College

Adam H. Greene, JD, MPH, Partner, Davis Wright Tremaine LLP

Gary W. Herschman, Member of the Firm, Epstein Becker Green

David Hoffman, JD, FCPP

President, David Hoffman & Associates, PC

Richard P. Kusserow, President & CEO, Strategic Management, LLC

Tricia Owsley, Compliance Director

University of Maryland Medical System

Erika Riethmiller, CHC, CHPC, CISM, CPHRM, CIPP/US

Chief Privacy Officer, Sr. Director Privacy Strategy, UCHHealth

Daniel F. Shay, Esq., Attorney, Alice G. Gosfield & Associates, PC

James G. Sheehan, JD, Chief of the Charities Bureau

New York Attorney General's Office

Debbie Troklus, CHC-F, CCEP-F, CHRC, CHPC, CCEP-I

Managing Director, Ankura Consulting

EXECUTIVE EDITOR: Gerard Zack, CCEP, CFE, CPA, CIA, CRMA
Chief Executive Officer, SCCE & HCCA
gerry.zack@corporatecompliance.org

NEWS AND STORY EDITOR/ADVERTISING: Margaret R. Dragon
781.593.4924, margaret.dragon@corporatecompliance.org

COPY EDITOR: Patricia Mees, CHC, CCEP, 888.580.8373
patricia.mees@corporatecompliance.org

DESIGN & LAYOUT: Pete Swanson, 888.580.8373
pete.swanson@corporatecompliance.org

PROOFREADER: Bill Anholzer, 888.580.8373
bill.anholzer@corporatecompliance.org

PHOTOS ON FRONT COVER & PAGE 12: Amelia Panico

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is \$295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to *Compliance Today*, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Copyright © 2019 Health Care Compliance Association. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means without prior written consent of HCCA. For Advertising rates, call Margaret Dragon at 781.593.4924. Send press releases to M. Dragon, 41 Valley Rd, Nahant, MA 01908. Opinions expressed are not those of this publication or HCCA. Mention of products and services does not constitute endorsement. Neither HCCA nor *CT* is engaged in rendering legal or other professional services. If such assistance is needed, readers should consult professional counsel or other professional advisors for specific legal or ethical questions.



Compliance Today is printed with 100% soy-based, water-soluble inks on recycled paper, which includes 10% post-consumer waste. The remaining fiber comes from responsibly managed forests. The energy used to produce the paper is Green-e certified renewable energy. Certifications for the paper include Forest Stewardship Council (FSC), Sustainable Forestry Initiative (SFI), and Programme for the Endorsement of Forest Certification (PEFC).

GOT PRIVILEGE? BEST PRACTICES TO PROTECT PRIVILEGES DURING AN INTERNAL INVESTIGATION

by James Holloway



James Holloway

(jholloway@bakerdonelson.com) is a shareholder in Baker Donelson's Washington, DC office, practicing in the Health/Government Enforcement & Investigations Groups.

Whenever a provider begins an internal investigation into a compliance concern—whether prompted by an employee complaint, a government inquiry, an audit, a media report, or other factors—the protection of legal privileges should be top of mind. Internal investigations typically involve candid and confidential discussions regarding a provider's failure to comply with regulatory requirements, standards of care, or policies. Sometimes there are internal discussions about the provider's awareness of past non-compliance and the failure to take corrective action. There are numerous cases in which a provider was hit with a large verdict or forced into making a large settlement payment, because the government or a private party was able to obtain highly incriminating internal documents that could have been validly withheld from disclosure if the provider had taken

the necessary steps to establish and maintain recognized legal privileges. That is an unforced error that providers should strive to avoid.

Common legal privileges for an internal investigation

Two legal privileges are usually available to protect internal investigations. The attorney-client privilege protects written and oral communications that are intended to be confidential between a client and their lawyer, and the privilege applies if a significant purpose of the communication is obtaining or providing legal services. Communications between the provider and its legal counsel during the course of an internal investigation could potentially be protected by the attorney-client privilege. The work product privilege protects materials prepared by or at the direction of a lawyer, for litigation or in anticipation

of litigation. In many cases, an internal investigation is conducted in anticipation of litigation, so the work product privilege may be available.

With any internal investigation, providers should have two related goals in mind. First, establish the privileges for internal communications and materials made during the investigation. Then protect those privileges by avoiding disclosures of information to outside parties that result in a waiver or loss of privileges.

Importance of privileges

Why should providers care about privileges? Because government regulators and plaintiffs' lawyers seeking to extract enormous payments from providers know that the provider's sensitive internal communications and records are likely the best evidence to prove any intentional, willful, malicious, or reckless non-compliance. Although providers may attempt to assert privileges to prevent the disclosure of such information, outside parties that have a financial incentive to push for the information may drag providers into court, where providers will have the burden of proving that privileges apply. Courts scrutinize assertions of privilege and do not hesitate to reject privilege claims that are not valid. In such cases, courts will compel providers to produce the information they attempted to withhold. And the forced disclosure of information that demonstrates a provider's non-compliance may have devastating consequences for the provider.

Therefore, it is critical to establish privileges at the outset of an investigation to make sure that information gathered throughout the course of the

investigation is protected. Providers must use a lawyer to assure that privileges apply, so either an in-house or outside lawyer should be involved from the beginning of the investigation. Although a communication with an in-house lawyer may be privileged, a provider's in-house lawyer sometimes functions in a business, non-legal capacity. Similarly, sometimes a provider's compliance officer is a lawyer, and the compliance officer may provide both business and legal services to the provider. In those instances, it may be more difficult to demonstrate that a communication with an in-house lawyer was for the purpose of obtaining or providing legal services on behalf of the provider. The involvement of outside counsel who does not serve a routine business function within the company makes it easier to prove that a significant purpose of confidential communications with a lawyer was obtaining or providing legal services for the provider.

Many internal investigations require the use of outside consultants, such as medical, billing, or accounting experts. Confidential communications with those experts, and the work product of those experts, may be protected by legal privileges if the experts are being used to assist a lawyer in the delivery of legal services to the provider. Thus, the experts should be retained by the provider's lawyer to demonstrate that the experts are working specifically to assist the lawyer with the delivery of legal services.

Misconceptions about privileges

It is important that information is protected by privileges upon its creation, because non-privileged

information created during an internal investigation cannot later be converted into privileged information. Thus, a provider that gathers information through its own investigation, before bringing in a lawyer, cannot make the information privileged simply by passing it on to a lawyer who is brought in later during the investigation. Although providers may be tempted to hold off using a lawyer unless and until damaging information is discovered during the investigation, that tactic will not assure that the information is protected by privileges.

...outside parties that have a financial incentive to push for the information may drag providers into court, where providers will have the burden of proving that privileges apply.

There are some other common misconceptions about using lawyers to create privileges. Having a lawyer join a meeting or including a lawyer in an email or memo will not by itself assure a privilege. Likewise, taking a communication between non-lawyers and forwarding it to a lawyer will not assure a privilege. Discussions at a meeting or in an email or memo cannot be protected by the attorney-client privilege unless the discussion involves a lawyer, the communication

is intended to be confidential, *and* a significant purpose of the communication is obtaining or providing legal services. Confidential materials prepared during an internal investigation and later given to a lawyer cannot be protected by the work product privilege unless the material was prepared by or at the direction of a lawyer, either in anticipation of litigation or for a pending litigation. Furthermore, labeling documents as “privileged” will not assure that they are actually privileged. A provider ultimately may be forced through a court proceeding to produce material labeled as “privileged” if it did not meet all the criteria for privileges to apply.

Avoiding waiver of privileges

Once a provider establishes privileges for information gathered during an internal investigation, it is important to avoid a waiver of the privileges through a disclosure of the information. An inadvertent disclosure of privileged information to outside parties may not necessarily waive applicable privileges, but an outside party seeking to obtain privileged information may argue to a court that the disclosure of the information was intentional, not inadvertent. It is not always clear whether a disclosure was intentional or inadvertent. Even when there is a disclosure that the provider believes

is inadvertent, there is a risk that a court will determine that it was an intentional waiver of a privilege.

One common risk of waiver is present when email strings are created and forwarded. An initial email communication between a provider’s employee and legal counsel may be privileged. However, as the email string grows with additional communications, eventually the email string may be forwarded to a recipient who should not be receiving privileged information, but the person forwarding the email string neglected to notice that an earlier email within the string was privileged. Although labeling an email as “privileged” will not guarantee that it is privileged, such labeling warns recipients of the email that it should be handled carefully because the author considers it to be privileged, which may reduce the risk of waiver from forwarding the communications to unauthorized persons.

The intentional disclosure of privileged information usually results in a waiver of the privilege. Sometimes a provider may consider a voluntary disclosure of privileged information to government regulators as a means to reduce the severity of punishment imposed by the government. There may be valid reasons to disclose privileged information, but it will likely waive applicable privileges. Thus,

providers should carefully weigh the pros and cons of disclosure with their legal counsel.

Furthermore, sometimes there are multiple providers involved in an investigation, and they may consider sharing privileged information with one another during the investigation under a joint defense or common interest agreement. Such agreements may be effective to avoid a waiver of privileges, but only if there is an actual common interest among the parties. Using an agreement that merely recites a common interest, when there actually is no common interest among the parties, will not assure that privileged information can be shared without a waiver. Because there is a risk that sharing privileged information with another party may not necessarily be protected by a joint defense agreement, providers should consult with legal counsel to evaluate whether a joint defense agreement will effectively protect the sharing of privileged information in a provider’s particular circumstances.

Conclusion

Providers conducting an internal investigation are entitled to assert valid legal privileges, but they must act carefully, in consultation with legal counsel, to assure that privileges are established and preserved throughout the investigation. ^{CT}

-
- ◆ Be sure to have in-house or outside counsel lined up at the start of an internal investigation.
 - ◆ Legal counsel should retain the experts who will be assisting with an investigation.
 - ◆ Label materials as “privileged” to alert recipients to safeguard the materials, but do not expect that label to protect non-privileged information.
 - ◆ Be careful when forwarding or sharing privileged information to avoid waiving privileges.
 - ◆ Disclosing privileged information outside the company should only be considered after consulting with legal counsel.