Compliance Today - June 2020
Establishing a best practice approach for your compliance, privacy, and security programs

By Kelly McLendon, RHIA, CHPS

Kelly McLendon (kmclendon@complianceprosolutions.com) is Managing Director at CompliancePro Solutions in Titusville, FL.

Healthcare compliance is based, in large part, on the Department of Health and Human Services (HHS) Office of Inspector General (OIG) model compliance programs,[1] which must be understood and implemented by all compliance officers working in healthcare. For example, the seven elements of a compliance program evaluation are based on Chapter 8 of the U.S. Sentencing Guidelines for Corporations.[2] Each organization must tailor the elements of model compliance programs that are similar to their needs to develop best practices for their compliance efforts. Best practices are a combination of rules, regulations, and the most efficient and effective ways of performing operations, whether manual or automated.[3]

The content published by OIG is presented as a series of voluntary compliance program guidance documents,[4] but they may also be a source of focus by OIG and other regulatory investigators as a part of their enforcement activities. The guidance is directed at various segments of the healthcare industry, such as hospitals, nursing homes, third-party billers, and durable medical equipment suppliers, to encourage the development and use of internal compliance controls to monitor adherence to applicable statutes, regulations, and program requirements.

Since the HHS model compliance programs are quite voluminous and complex, a good place to start is with a discussion of key elements and their best practices. From there, one can progress into increased granularity by illustrating some of the requirements for the specific areas of privacy and security that deal with compliance assessment, which provide guidance about related best practices. The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules[5] call for conducting both privacy and security program assessments to create a best practice standard for how privacy and security compliance is managed.

Seven elements of the OIG model compliance program

The following elements have been identified by OIG as areas of focus for assessment and evaluation of compliance programs.[6] Ensure they are addressed when assessing, measuring, and evaluating compliance program elements.

- “Implementing written policies, procedures and standards of conduct;
- “Designating a compliance officer and compliance committee;
- “Conducting effective training and education;
- “Developing effective lines of communication;
- “Enforcing standards through well-publicized disciplinary guidelines;

- “Conducting internal monitoring and auditing; and
- “Responding promptly to detected offenses and developing corrective action.”

Measuring compliance program elements is mandatory under virtually all compliance rules and regulations. In order to facilitate a best practice approach, start with defining expectations of performance or standards for each element. Then, devise assessments or audits to measure and report the results while paying attention to any variances.

For example, a standard for compliance education may be that every senior leader should receive two hours of training annually. If there are 20 senior leaders, and 16 achieved the standard, it’s a 75% achievement rate. Report the reasons for the variance within proper governance channels with a year-to-year comparison of results and a plan for remediation. The following year asses it again to determine if the remediation actions have been successful and tweak further if needed.

OIG model compliance program key element best practices

The U.S. Department of Justice guidance titled *Evaluation of Corporate Compliance Programs*[7] offers useful information about how it reviews and assesses compliance programs looking for violations. This guidance is not healthcare-industry specific, but it is illustrative of the elements used for compliance program evaluations. The following items show where the Department of Justice’s attention is focused. Compliance program governance must address each of these areas with organized best practices.

- Analysis and remediation of underlying misconduct,
- Conduct of and commitment by senior and middle management,
- Stature of the compliance function,
- Autonomy of the compliance function,
- Compliance program funding and resources,
- Corporate response to expressed compliance concerns,
- Process for responding to findings,
- Disciplinary action consistency,
- Risk management process,
- Frequency of updates to policies and procedures, and
- Whether direct reporting of compliance violations to the board of directors is established and possible.

Compliance governance

An overarching governance structure must be put into place within any organization that has governmental rules and regulations with which they must comply.[8] Typically, governance is managed by senior-level administration, with the required compliance departments and staff size appropriate for the organization’s size. It is mandatory to adequately staff company compliance programs—failure to do so is a violation of multiple rules.

One best practice—for organizations that are large enough to warrant it—is having a compliance committee. Membership should be established with senior leaders, including the CEO. The chief compliance officer (CCO) should chair the committee and recognize quorum's requirements. Detailed minutes of the required regularly scheduled meetings should be taken. Meetings should be scheduled monthly or quarterly and occur with established ground rules. Compliance committees should establish a charter that reflects thoughtful development to guide their operations.

All organizations with compliance responsibilities should have an appointed CCO. Typically, these organizations will have multiple compliance efforts to manage the need for a single point of leadership. The CCO has several best practices associated with the role, many of which can be incorporated into the job description. Examples include:

- The CCO should be able to make proper decisions without fear of retaliation.
- *The lead admitter of patients to the hospital is in violation of the medical records completion policy*. The CCO should be able to revoke privileges as policy states.
- *The CEO's spouse is asking to review sensitive and confidential information related to an upcoming community fundraiser.* The CCO should be able to treat her as if she were a normal citizen.
- The CCO should be independent and report directly to the board.

The CCO should be a subject matter expert and have certifications proving their validity, as well as a list of conferences attended, presentations made to industry, etc. However, no one in this business knows everything. It is ok to ask for help. Is the CCO able to get help when it is needed? For example, a CCO may need a subject matter expert in coding and reimbursement issues, which can be notoriously complex. Are they able to get one?

Best practice compliance elements

Although there are numerous areas of compliance that can have best practices applied to them, this article will focus on the following best practice areas for compliance:

- Hotline calls,
- Education,
- Audit preparation,
- Potential trends in coding and billing results,
- Annual audit work plan completion,
- Budget analytics, and
- Other data points to trend by year.

Hotline

Hotlines and online incident reporting can take many forms. Some organizations have more generalized reporting, and others are more specific (e.g., privacy incidents may be reported through a web form separate from general compliance reporting). Regardless of the methods and automations chosen, ensure that the calls and reports are all adequately logged into the appropriate central locations and worked on until their completion.

The results of hotline and other calls and reports of incidents must be reported in appropriate detail to governance. These reports are crucial to formulating corrective action plans and ways to continually achieve improvement. Sometimes they are derived manually, but it is becoming increasingly unsustainable with the complexities of modern compliance, so the use of automation has slowly taken over the reporting and measurement of the important metrics. The simplest compliance management and reporting now comes from spreadsheet-based processes, but there has been an increasing amount of automation of incidents and their reporting in the marketplace, which is making manual management of compliance untenable. Data to evaluate include how many of those incidents and reports resulted in investigations, reportable breaches, remediations, mitigations, disciplinary actions, or other actions.

Education

How much compliance education is enough? Usually, most parties understand that some education must be provided to facilitate compliance, but the question becomes, "How much education is enough, and how should it be delivered to be successful and to not become repetitious and burdensome, which can reduce the training's effectiveness?" At times, there could be OIG corporate integrity agreement-based requirements, but otherwise, a best practice must be established. The training program that is decided upon should have the support of the board of directors. For example, staff (except housekeeping and food service) can be obligated to receive an hour of training annually. Executives, physicians, and the board should receive two hours of training annually. And those involved in negotiating physician or referral arrangements should receive two hours of training annually with specific training on the Stark Law and the Anti-Kickback Statute by an expert.

Another way to measure your organization's compliance culture is to ask, "Can your organization tolerate this?" It is a basic expectation of OIG that a culture of compliance be established, educated upon, and implemented by all workforce members. Although those specific training guidelines[9] are suggestions for best practices, your organization may vary them but should always have adequate justifications for the duration, frequency, and content of all workforce member training programs.

Board education and reporting is one of the most important aspects of free-flowing information from all levels of the organization to the top. These reports should be tailored to what is occurring—internally and externally—and should address associated risks—organizational and personal. The CCO should be able to communicate with the board whenever they want without hesitation—often, they report to the board.

Important questions to ask about a compliance program's governance include:

- Are board members involved in the compliance program's oversight? What is the compliance knowledge level of the board?
- Can the CCO get assistance (externally) when they deem it necessary?
- What is the frequency and quality of the information flow?
- Is the board receiving all necessary information?

Audit, assessment, and evaluation monitoring

The purpose of auditing, assessing, and monitoring is to continually look for areas to improve, as well as detecting violations or problem areas as soon as possible. In today's information technology (IT) world, there are many forms of automated monitoring of systems and data, some of which get routed to the compliance staff, and some are managed by IT security or others. Regardless of who works on resolving the issue, the alerts monitoring systems can produce summaries, numbers, and trends that should be reported through appropriate channels at whatever granularity is needed to facilitate information flow without being overly burdensome. Consistent measurements are a must.

Fifty claims randomly selected in a probe sample is consistent with OIG requirements. Five percent or below is an acceptable error rate.

Annual workplan completion

It is a critical part of compliance to produce a work plan approved by the compliance/audit committee or board annually. Again, these have typically been presented as a spreadsheet-based manual set of processes, which are now migrating to online versions with automation. Trend the results of the following questions to serve as resources for accurate planning.

- How many projects were on the original plan?
- How many projects were added during the year?
- How many were completed? How many were not?
- How many internal (and external) corrective action plans are in place?
- Are the unresolved work plan items due to the budget, operational, or other issues?

Budget analytics

Budget analysis should be based on operating and full-time equivalent (FTE) budgets approved by the board or compliance/audit committee. Although there are a lot of data that can be reported, making the budgets understandable is also important. Data that should be reported may include:

- Operating budget variance (dollar amounts and percentages),
- An explanation for any variance,
- FTE budget variance (dollar amounts and percentages),
- An explanation for any turnover,
- An explanation for any unfilled vacancies,
- A proposed corrective action, and
- Trending of budgets and actual expenses over the past several years.

Good management dictates that departments and staff operate within an acceptable budget, but that doesn't mean the organization is doing a good compliance job.

Privacy and security compliance assessment

Assessing compliance privacy and security has become more complex. The increased number of state and federal rules and the expanded attention on these areas have combined to place additional scrutiny and risk upon the privacy and security officers and their compliance staff. It's important to be vigilant and proactive not only in security and cybersecurity, but also within access and privacy operations. It bears remembering that patients have privacy rights (e.g., amendment, restriction, access) that they request constantly, and any failures in this area can result in an Office for Civil Rights (OCR) investigation. Assessment of both security[10] and privacy[11] compliance must be undertaken on a regular basis. The HIPAA Security Rule requires a National Institute of Standards and Technology (NIST) security risk analysis to be performed on an ongoing basis, with appropriate risk management and a remediation plan for all systems that contain patients' protected health information. Although these analyses are an ongoing exercise, they are typically renewed annually.

The HIPAA Privacy Rule is not as prohibitive in assessment requirements, but it can be inferred through the rules, guidance, and enforcement actions that the privacy compliance program should also be assessed—in a risk format or not. This HIPAA privacy assessment requirement has now expanded, with the new General Data Protection Regulation (GDPR) and California Consumer Protection Act (CCPA) rules acting to make more information reside under the compliance programs' umbrella. The number of state and federal privacy and security rules is continuing to increase, so watching for areas to update within a compliance program is always required.

Of the seven elements of the OIG model compliance program, four can be partially addressed through the use of assessments. Data collection is part of the audit requirements, along with policy and procedure evaluation and corrective action mitigations. Reporting on these items serves to provide the compliance program oversight.

A robust and widely scoped privacy compliance program assessment will include the following areas of review and evaluation:

- Details about the organization's privacy compliance program,
- Privacy (and breach) policies and procedures and communication,
- Patients' rights,
- Workforce privacy training,
- Designated record sets,
- Incident management and breach notification,
- Incident history,
- Business associates' management (through satisfactory assurances/questionnaires), and
- Research.

Similarly, the required areas of review and evaluation within a HIPAA security risk analysis include:

- Policies and procedures to prevent, detect, and correct security violations and define appropriate sanctions;
- Assigned security responsibility (i.e., security officer and governance);
- Appropriate and authorized access to protected health information and clear termination procedures (and deprovisioning of access);
- Security awareness and training for entire workforce;
- Security incident procedures;

- Contingency and backup plans;
- Periodic evaluation and monitoring of security compliance with continual feedback and remediation;
- Business associates' compliance (through satisfactory assurances);
- Facility access controls;
- Workstation use and security;
- Device and media controls;
- Access controls;
- Audit controls;
- Integrity;
- Person or entry authentication; and
- Transmission security.

Assessments of compliance are rarely stand-alone; certain other supporting documentation is required for full compliance. The following are increasingly required as a part of IT and compliance:

- Policies and procedures (e.g., HIPAA privacy can have 20 to 25 policies, with another 20 to 25 for security), which should accompany compliance assessments, as many of the questions will be based on current policies and procedures;
- Documentation of IT hardware and software assets and their associated security controls;
- Data asset cataloging with or without data flows (OCR has said that this is a crucial part of security and privacy management—both GDPR and CCPA require them—built upon governance, record, and legal record management standards and best practices);
- Data flow mapping (can be visual—made in Microsoft Visio—or part of a data catalog); and
- IT asset management, including organization of controls, safeguards, and other details like software versions.

Best practices for privacy audit/assessment and monitoring include regularly scheduled privacy compliance assessments. Such an assessment can be an overview of the entire privacy program or focused areas, such as patient access vs. disclosure audits or response times and results of amendment requests. Automation is also useful in monitoring privacy incidents and whether they are corporate policy and/or reportable breaches to OCR and state governments—their reporting can become more readily used for trending and analysis of the effectiveness of both the privacy and general compliance programs. Similarly, security compliance must be assessed in a prescribed risk-based manner, combined with cybersecurity controls and active monitoring and alerting. Security incident management and reporting has become well automated, which is needed to operate sophisticated systems that contain patient and other personal information with the lowest amount of risk possible.

Assessment areas within both privacy and security are not limited just to HIPAA; other rules and requirements drive assessment of privacy and security compliance, and this list is growing steadily with late additions like the

GDPR and CCPA. Examples of different assessments that may be required include the following.

Privacy assessments:

- Privacy risk analysis: general, advanced, and audit levels (for covered entities or business associates);
- Privacy and security walkthrough assessment;
- Ongoing staff privacy and security questionnaires;
- Business associate agreement component assessment; and
- Business associate privacy and security compliance assessment (satisfactory assurance).

Security assessments:

- Security risk analysis: general, advanced, and audit levels (for covered entities or business associates);
- NIST cybersecurity framework;
- Payment card industry data security standard assessment (credit card security);
- IT asset management questions; and
- Defense Federal Acquisition Regulation Supplement NIST 800-171 (non-classified federal data) assessment.

Takeaways

- The seven elements of the Office of Inspector General model compliance program are important foundational components for any compliance program.
- Likewise, the *Evaluation of Corporate Compliance Programs* clarifies compliance enforcement, offering insights into details to be addressed within these programs.
- Compliance governance must be organized, properly staffed, provided tools needed for success—including automation—and well managed.
- Hotline calls, education, work plans and audit preparation are a few of the items that represent best practices used to meet regulatory compliance requirements.
- Assessing privacy and security compliance is required and is often addressed with dozens or hundreds of questions across the entire scope of the rules being evaluated.

[1] Publication of the OIG "Compliance Program Guidance for Hospitals," 63 Fed. Reg. 8987 (Feb. 23, 1998).
[2] U.S. Sentencing Guidelines Manual § 8 (U.S. Sentencing Comm'n 2018).
[3] Kelly McLendon and Bret S. Bissey, "Establishing A Best Practice Approach for Your Compliance, Privacy and Security Programs," presentation, 2020 Managed Care Compliance Conference, January 2020.
[4] "Compliance Guidance," HHS OIG, last accessed April 15, 2020, https://bit.ly/34FpMR2.
[5]45 C.F.R. § 164.
[6] Publication of the OIG Compliance Program Guidance for Third-Party Medical Billing Companies, 63 Fed. Reg. 70,138 (Dec. 18, 1998).

[7] U.S. Dep't of Justice, Criminal Div.,*Evaluation of Corporate Compliance Programs* (Updated April 2019), http://bit.ly/2Z2Dp8R.
[8] HHS OIG, Association of Healthcare Internal Auditors, American Health Lawyers Association, and Health Care Compliance Association, *Practical Guidance for Health Care Governing Boards on Compliance Oversight*, April 20, 2015, https://bit.ly/3ahysOP.
[9] HHS OIG, *Measuring Compliance Program Effectiveness: A Resource Guide*, March 27, 2017, http://bit.ly/2OTDr0C.
[10] 45 C.F.R. § 164.308.
[11] 45 C.F.R. § 164.530.