Compliance Case Studies

What Can Go Wrong
and
How Can We Learn from Others?

Caron Cullen, Sr. Vice President & Compliance Officer, Affinity Health Plan

Virgilio Florentino, Principal, Compliance Strategies, Inc.

Objectives

- Discuss actual compliance issues from unidentified Health Plans
- Share how the compliance issue was discovered
- Review what immediate actions were taken
- Identify all required notifications
- Examine the lessons learned from the incident
- Evaluate what may have been done differently to prevent the compliance issue, if possible, in the future
- Discuss Best Practices from these compliance experiences

What else would you like to know?
Case Study #1 – HIPAA Breach

- Plan receives an anonymous letter regarding a whistleblower allegation of a third party vendor.
- Investigation is completed using an independent external law firm.
- Good news – the Whistleblower allegation is unfounded.
- Bad news – during the investigation, the external investigator identifies a HIPAA breach in the third party vendor’s former employee’s email account.

What do we do?

Case Study #1 – And the answer is...

- Investigate the individual’s emails.
- Findings – Emails with Member data was sent to a non-employee to help format the document
- Affect – Of course, over the magic number of 500 Members were affected.
- Actions – Contact former EE and brother to determine what they did with the data.
- Resolution – Notification process to members, regulators. letter, toll free number, CS scripts, etc.
Case Study #1 – Lessons Learned

- Do you know what your FDRs have in place to protect your member data?
- Do you have a new Business Associate Agreement with the requirements of HITECH – more responsibility for the FDR?
- How much flexibility do you have to mandate certain elements in a corrective action plan? What, does your contract allow?
- What type of auditing and monitoring do you do? Does you include HIPAA Privacy and Security reviews? Do you perform on-site reviews?
- Are employees afraid to ask for training? Why?

Case Study #2 – Claims Fraud

- Plan receives a tip regarding an employee in the Claims Department.
- The employee allegedly processed a fraudulent reimbursement claim.
- Other employees may have been involved in the operation.

What do we do?
Case Study #2 – And the answer is…

- Determine the validity of the allegation. Is this a retaliation against another employee?
- Finding – Claims employee worked with another employee in the department to falsify a reimbursement to a family member, intercepted the check, and transferred the funds into own account.
- Affect – No other member reimbursements involved.
- Actions – Review internal controls, Increase checks and balances and limit access going forward.
- Resolution – Terminate employees and self disclosed to CMS, MEDIC, and local authorities.

Case Study #2 – Lessons Learned

- Do employees feel comfortable coming forward without fear of retaliation?
- What safeguards can you put in place to segregate duties? Have an internal audit performed to review.
- Did staff in that area get training about Conflicts of Interest and ramification for non disclosure?
- What monitoring tools can you use going forward?
Plan receives a tip regarding employee submitting fraudulent time sheets.

Plan utilizes a unique identifier (hand print) to clock in and out. Based on this, time sheets are printed, signed, and approved for payroll payment. However, employee allegedly found a loophole in the process.

Others may have been involved in the operation.

What do we do?

Compliance Officer identified specific dates when employee was on vacation.

Findings – Time sheet indicated she worked on days she was on vacation. Investigation determined employee scanned time sheet and used a program to pasting different hours.

Affect – One other employee was involved, a room mate.

Action – Added watermarks and other printing challenges.

Resolution – Self-disclosed to CMS and local legal authorities.
Case Study #3 – Lessons Learned

- Does your Compliance Department, and staff, live with an open door policy? Is your physical door open?
- Does the organization review existing processes and continually evaluate whether additional safeguards should be implemented?
- Does the organization keep abreast of new technology and integrate into its annual risk assessment of the organization?

Case Study #4 – Marketing Issue

- Plan’s monitoring reveal an increase in Beneficiaries complaints claiming they never enrolled in the Plan.
- Beneficiaries confirm the information on the Election Form (i.e., Name, address, HIC Number, etc.) were accurate.
- Beneficiaries confirm the signature on the Election Form belonged to them.
- None of the Beneficiaries ever met with a Representative of Plan.
- Many recall shopping in a grocery store on the date of enrollment.

What do we do?
Case Study #4 – And the answer is…

- Trend data. All Beneficiary complaints involved Sales Representatives in a specific area.
- Findings – Beneficiaries were offered a free chicken. Need to present Medicare Card, complete some questions, and sign acknowledgement. Beneficiary was actually signing an Election Form!
- Affect – Contacted 100% of enrollees from a specific Supervisor. Identified additional cases.
- Actions – Voluntarily mandated a more comprehensive verification process.
- Resolution – Self disclosed to CMS and State Licensing Board.

Case Study #4 – Lessons Learned

- Do you regularly monitor your Complaints, Grievances, and Appeals, especially if you see a variance in numbers?
- How do you drill down to see patterns and trends?
- How do you monitor Marketing Representatives and Agents? Secret Shoppers in the field? How often is enough?
- Do you provide marketing guidelines training and ensure each Representatives is aware that he/she is solely responsible for his/her action(s)?
- Make sure Compliance has authority and consistently exercises such authority. No exceptions for the high producer.
Case Study #5 – Credentialing Abuses

- Senior Manager receives allegation that the Credentialing Director was fraudulently obtaining provider signatures.
- Senior Manager performs independent investigation and obtains written statements from ex-employees.
- Compliance Officer works with FWA to perform investigation. Investigation lasting over nine months!
- During investigation, an anonymous email is sent to CMS indicating inappropriate conduct by Plan.
- MEDIC gets involved; Senior Manager resigns after the first day of investigation.

What do we do?

Case Study #5 – And the answer is...

- Finding - Employees scanned signatures from a valid contract and superimposed signature to recredentialing attestation. However, investigation provides no root cause of the activity.
- Board kept abreast of investigation. But a case was being concurrently investigated on Senior Manager harassment Credentialing Director.
- Affect – Over 800 recredentialing files were potentially modified.
- Actions – Plan voluntarily recredentialled affected files again. Removed computer program from all internal computers. Terminated entire department.
- Resolution – Plan terminates entire department but does not do so timely warranting inquiries from Program Integrity.
Case Study #5 – Lessons Learned

- Board informed of the FWA case but was not trained on responsibilities. Should the Board disclose the HR case to the FWA and/or Compliance Officer?
- Senior Manager was not trained on compliance and his role in an investigation (i.e., performing an independent investigation was harmful to the case).
- Initially informed CMS but failed to continually update Plan Manager on status. Additionally, updates provided to CMS verbally.
- The severity of allegation and length of investigation should have warranted a self-disclosure to MEDIC.
- Compliance Officer should have owned the case and followed up.

Best Practices – Audits

- Notification Letter – Understand what auditors want and when it’s due. Make it count, this is a first impression.
- Who’s Coming – Know your auditors, experience, and expertise.
- Roles and Responsibilities – Don’t leave anything to chance, discuss audit to the entire Organization and FDRs. Be prepared!
- Evaluating Effectiveness – Based on the notification, be prepared for interviews and supporting documentation
- Deliverables – Expect requests at any given time throughout the audit

*What else would you suggest?*
Best Practices – Compliance Officer

- The Compliance Officer is visible and available.
- Have an open door policy – listen and learn – from employees and other stakeholders.
- Make sure the Compliance Officer, and the compliance staff, has the appropriate qualifications to do the job.
- Participate in operational meetings to hear what is going on in the organization.
- Make sure your activities are publicized in many ways – departmental meetings, newsletters, walk-around the building, etc.

*What else would you suggest?*

Best Practice – Compliance Plan Review

- All plans discussed have a good Compliance Program. Is it enough?
- How do you take the Compliance Program to the next level?
- Examine the compliance issues at your organization for a year. What can you and the organization change?
- Consider having Internal Audit or an external consultant review what you have in place.
- Make sure the Compliance Officer, and the compliance staff, has the appropriate qualifications to do the job.
- Publicize issues and concerns regularly... monthly, quarterly, during National Compliance & Ethics Weeks so that compliance is front and center in the organization.

*What else would you suggest?*
Best Practice – Get the Leaders on Board

- Compliance is everyone’s responsibility!
- Constantly foster a culture of compliance.
- This includes the Board of Directors, the Executive Team, and Sr. Management.
- You need to have their support and commitment to make it happen.
- Convince the leadership it is much more cost effective to obtain the resources you need before an issue rather than after an issue (fines, penalties, cost of reputation, and corrective action plans).

What else would you suggest?

Best Practices – Self Disclosure

- If you identify something, that is good news! Your Compliance Program is working!
- Strongly recommend that you self-disclose issues to your regulatory agencies… State, Local, Federal levels including: State Department of Health, Department of Insurance, Office of the Medicaid Inspector General, Fraud Control Units, CMS, etc.
- Create and share your self-imposed Plan of Correction.
- Health Plans are harder on themselves then the government may be. Make sure it is extensive and it is implemented! If you say you will do it, you must do it!
- You and your program can shine as effective.

What else would you suggest?
### Best Practice – Third Party Vendors/FDRs

- Your Compliance Program is great but what are you doing to make sure your third party vendors/FDRs have one, too?
- Perform on-site visits at least once a year.
- Review their Code of Conduct and ensure they verified employees against OIG/GSA lists.
- Test one aspect, i.e., employees, including Board of Directors, have been trained. If you identify an issue, ask more questions and do more testing.
- Standardize auditing and monitoring approach. What Policies and Procedures are important to obtain?
- Do they have reports of a HIPAA breach or other compliance issues that you need to be aware of? If it is HIPAA, you as the covered entity need to know. If it is other types, perhaps not... do you agree?

*What else would you suggest?*

### Best Practices – Training & Education

- Do you have general and specific training for various areas and departments?
- When you have training, can you prove it, regardless of method?
  - On-line
  - Stand-up
  - Combination
- Does your training rosters contain: Date, Time, Location, and Facilitator?
- What are the Facilitator’s qualifications?

*What else would you suggest?*
Best Practices – CGA

- Review a sample of Complaints, Grievances, and Appeals (CGA)
- What does the review tell you?
  - Patterns and Trends
  - Timeliness
  - Regulatory Requirements
- How can you use this information to improve the process?
- What forum can you use to filter it to the operational areas since change is the responsibility of the operational areas not compliance?

What else would you suggest?

Best Practices – Audit vs. Monitor

- Understand the difference between auditing and monitoring.
- When you monitor, you are looking for trends, variances, anomalies in the data and information.
- If you find them, then you audit the process to identify if the trend, variance or anomaly represents a concern or weakness in the process.
- What is the balance of what you must do vs. what you would like do with the limited resources?
- How do you select and perform audits? Items on a three year cycle?

What else would you suggest?
Summary

Strive for 100% compliance at all times but can you prevent everything?

- Be realistic! Understand that STUFF happens even with a great compliance program.
- When something happens, react in a cool and calm manner!
- Manage it appropriately; implement corrective actions; and mitigate future risks.
- Always remember to lead the organization by your example... and remember the Compliance Professional’s Code of Ethics.

Questions

Time for your Questions!
Contact Information

Caron Cullen, Sr. Vice President & Compliance Officer
Affinity Health Plan
cullen@affinityplan.org

Virgilio Florentino, Principal
Compliance Strategies, Inc.
virgilio@costeam.us