Leveraging Internal Audit & Forensics In Your Compliance Program

April 17, 2018

Donald A. Sinko, Chief Integrity Officer
Vicki R. Bokar, Senior Director,
Corporate Compliance

Agenda

- Cleveland Clinic at a Glance
- The Integrity Office
- Case Studies
- The Case for Collaboration
- Areas of Benefit

Cleveland Clinic at a Glance

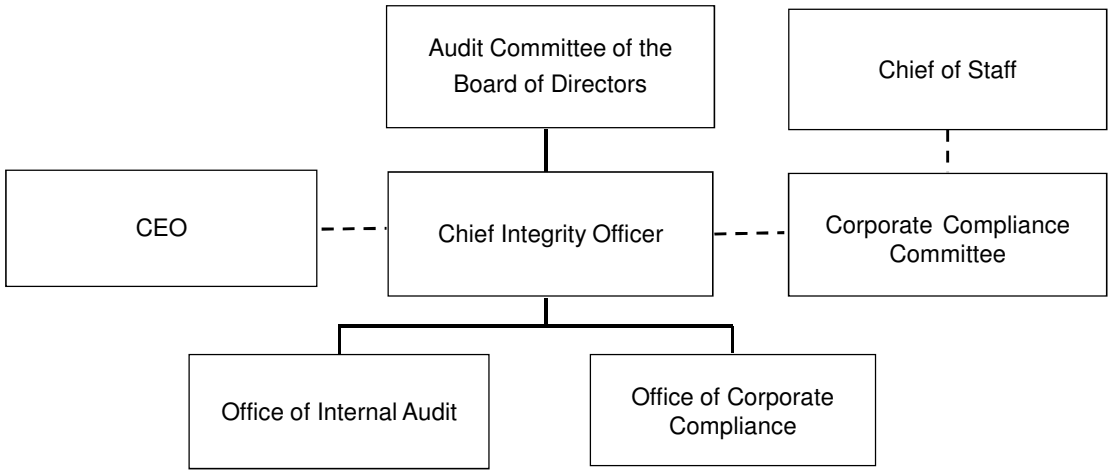
- 51,500 caregivers
- 7.1 million patient visits
- 220,000 hospital admissions
- 3,600 physicians & scientists
- 1,960 residents & fellows
- 10 Regional Hospitals
- 150+ Northern Ohio Outpatient Locations

3

Cleveland Clinic Locations

4

Cleveland Clinic's Integrity Office



5

Independence

- Is achieved through direct reporting (to the Board) and Integrity Office structure
- Eliminates real or perceived conflict of interest
- Does *not* mean Audit and Compliance cannot have close working relationships with business units (or with each other)
- Allows Audit and Compliance to gain access to any information needed to fulfill their responsibilities

6

The Controversy of Collaboration

- Different interpretations of what it means to be "independent"
- Some feel it prevents Internal Audit (IA) from independently auditing Compliance Program activities
- Some of these views are driven by corporate culture, politics, differing agendas
- Compliance and Audit have not always been aware of the subliminal internal and external forces that have helped to shape these interpretations
- There is much more overlap than anyone will care to admit (especially in health care)

7

Case Study #1

- Jane Doe contacts a Customer Service Representative (CSR) to complain that she has been turned over to collections for emergency room services that she never received
- Jane tells the CSR that her SSN is 123-45-6789
- The CSR reviews Jane's account and discovers that her SSN is mistakenly recorded as 123-45-678*8*
- A search using Jane's correct SSN shows that 123-45-6789 is associated with the account of patient Alice Smith
- Further review of Alice's account shows that she received emergency services for the dates in question

**All names and identifiers are fictitious

8

What is the Most Likely Explanation?

A. An employee made a keystroke error when registering Jane Doe
B. Jane unknowingly transposed the last two digits when stating her SSN at the time of registration
C. An employee intentionally transposed the SSN as part of elaborate scheme to obtain narcotics
D. The incorrect SSN's originated from human error that was perpetuated through an interface with downstream systems

9

Initial Findings

- Jane Doe's account contains a scanned copy of her insurance card with the correct SSN (123-45-6789)
- Alice Smith's account contains no identification cards
- A demographic change report shows that Jane Doe's account was edited on 1/5/17 by a unit secretary named Alicia Smyth

10

Things Aren't Always as They Seem

11

More Interesting Findings

- A user audit is generated for employee Alicia Smyth to better understand her actions at the time she accessed Jane Doe's account
- The audit reveals that Alicia made no other changes to Jane's account
- The audit reflects Alicia accessed records of several different patients; each having very similar first and last names (e.g. Aliah Smith, Acacia Smith, Aleeshia Smyth etc.)
- All of these patients received emergency services

12

Collaboration Helps to Connect The Dots

- Dates of Service
- Check-in; check-out times
- Emergency phone contacts
- Prescription records
- Forensic reconstruction of Employee's actions while logged into the EMR system
- Kronos data (time clock)

13

Case Study #2

- Anonymous hotline call alleges an employee has impermissibly accessed the EMR of a co-worker and disclosed highly sensitive information to other persons
- A chart audit reflects limited access by two different employees
- Both employees are assigned to a different unit than that of the "co-worker" whose PHI was allegedly disclosed
- There is no evidence to suggest that either employee was ever involved in the provision of health care to the co-worker

14

Interviews

- Employee 1 adamantly denies the access was hers. Denies any familiarity with the patient in question
- Employee 2 admits to having formerly worked with the co-worker, but insists that someone else must have accessed the record under his login credentials. Admits he sometimes forgets to log off his workstation

15

What is the Most Likely Explanation?

A. One or both employees are lying and impermissibly "snooped" in the co-worker's record
B. Someone fraudulently obtained the login credentials for one or both employees and accessed the co-worker's record
C. One or both employees forgot to log-off a workstation, which allowed an unauthorized person to impermissibly access the co-worker's record

16

You've Probably Heard it Before . . .

- "The audit trail is wrong. I never looked in that person's record."
- "I must have forgotten to log-off my workstation and someone else accessed the record under my login."
- "Someone must have stolen my credentials and logged in as me."

17

Things Aren't Always as They Seem

18

Audit Logs Are Just Evidence

Timestamp (Local)	User Name	User ID	Event	Event area	Type	Patient Na	MRN	Patient ID	Encounter	Associated Data
			Patient SnapShot viewed	Patient Clinical Info	View				N/A	Report viewed CCF PATIENT SNAPSHOT (RICH TEXT) [2018054]
			Patient SnapShot viewed	Patient Clinical Info	View				N/A	Report viewed CCF PATIENT SNAPSHOT (RICH TEXT) [2018054]
			Patient Selected From Patient Lookup	Patient Demographics	View				N/A	From duplicate warning No

19

Time to Collaborate

- Standard audit trails do not always reflect what actually occurred
- Forensic auditors capture and interpret network data, providing more objective evidence of a user's behavior
- This additional evidence often incriminates, but in some cases exonerates the person under investigation

20

Collaboration Cracks the Case

- Two heads are better than one
  - Compliance: “I wonder if ….”
  - Audit: “I know where we can pull data for that”
- Examples:
  - Nurse locator data (Hill/Rom)
  - Workstation reports
  - EMR session data collected by forensic software

21

Forensic Evidence

- User did a specific look-up search by the employee’s first and last name
- Search yielded 27 results with same first and last name
- User selected the record belonging to the co-worker and added this to his “patient list”
- User deleted the co-worker from the “patient list” an hour later

22

Collaboration Makes Sense

- Joint investigations promote objectivity, impartiality and fairness
- Collaboration improves the quality of work in both departments and provides management with even greater decision-making support
- Collaboration allows compliance & audit to share nuances of day-to-day business operations, which enhances the ability of both departments to prevent and detect risk

23

Collaboration at Cleveland Clinic

- Compliance & Audit are both independent of management (neither has a stake in the outcome of the investigation)
- Allows expanded access to tools, techniques, specialized skills and knowledge of operations
- Both departments already have an obligation to protect the integrity and confidentiality of the investigation

24

Collaboration is Not Limited to Investigations

Internal Audit can support monitoring & auditing activities of the Compliance Program

- EMTALA
- Provider contracts
- Conflict of interest
- Effort reporting
- Data at rest/Data in motion
- ABNs
- Research billing
- Many, many more

25

Collaboration in Risk Assessment

- The IA risk assessment process differs from that of compliance, but helps to expose risks that might not have been identified by either process alone
- IA can provide validation that controls are working (or not), which in turn helps compliance conduct more effective monitoring of responsible business units

26

As Risks Evolve, the Value of Collaboration Will Increase

BECKER'S
HEALTH IT
& CIO REVIEW

1 in 5 health employees willing to sell confidential data: 7 survey insights

Written by Julie Spitzer | March 02, 2018 | Print | Email

Nearly one in five healthcare employees would be willing to sell confidential data to unauthorized parties for as little as $500, according to a survey from Accenture.

For the report title "Losing the Cyber Culture War in Healthcare," Accenture surveyed 912 provider and payer organizations across the U.S. and Canada.

Here are seven survey insights.

1. About 18 percent of respondents said they would be willing to sell confidential data — such as login credentials, installing tracking software and downloading data to a portable drive — to unauthorized parties for as little as $500 to $1,000.

2. About 24 percent of respondents said they knew of someone in their organization who sold credentials or access to an unauthorized outsider.

27

Cleveland Clinic

Every life deserves world class care.