

# Inside Criminal Minds, Part I

by Allan P. DeKaye, MBA, FHFMA

*Fraud! Settlements! Restitution! Jail time! All headlines ripped from industry trade journals and newsletters. The unsettling fact is that these same headlines have appeared with regularity over the last 15 years, or at least since Health Care Fraud has become a target of investigation at the federal, state and local levels.*

**Inside Criminal Minds**, presented in two parts, takes a closer look at those who have committed fraud, and examines the characteristics that may have led to this criminal behavior. It also will look to define varying degrees of greed, as behavioral traits common to the criminal mind. In addition, the article will examine: (1) the way many compliance structures work to detect and prevent fraudulent activities to see if it provides sufficient safeguards, (2) the more sophisticated data models used to guard against identify theft and record breaches, and (3) the way we screen new hires and reevaluate existing staff to see if lapses or loopholes exist that threaten to exploit vulnerable areas. Finally, the article will present related perspectives and vantage points to address compliance concerns.

## The Hierarchy of Need

History has a way of repeating itself: climate, war, disease, crimes and behavior, to mention a few illustrations. In 1954, Dr. Abraham Maslow introduced the “Hierarch of Needs.”<sup>1</sup>

In this classic work, Maslow identifies five needs: physiological, safety, social, esteem, and self-actualization. In its purest sense, Maslow’s approach contends “...Humanists do not believe that human beings are pushed by mechanical forces, either of stimuli and reinforcements (behaviorism), or of unconscious instinctual impulses (psychoanalysis). Humanists focus upon potentials. They believe that humans strive for an upper level of capabilities...”<sup>2</sup>

Over the years, Maslow’s “needs” theory has been expanded and adapted. For example, the need for “safety” can be translated to include “...our urges to have a home in a safe neighborhood, a little job security, and a nest egg ...and so on.”<sup>3</sup> With this in mind, another adaptation states: “If Maslow’s theory is true, there are some very important leadership implications to enhance workplace motivation.” To allow workers to reach Maslow’s self-actualization level, “...[the workplace needs to] offer challenging and meaningful work assignments which enable innovation, creativity and progress according to long-term goals.”<sup>4</sup>

“Maslow’s concept of self-actualization relates directly to the present day challenges and opportunities for employers and organizations – to provide real meaning, purpose and true personal development for their employees. For life – not just for work.”<sup>5</sup> While Maslow provides one model for understanding what individuals need, then we need to examine where in the workplace either needs are not being met, or additional behavioral characteristics can be identified to determine if an early warning to predisposition to criminal behavior is possible.

While a psychosocial profile might define a potential criminal from an accounting profile, other characteristics also might be identified. In the Accounting Department at Louisiana State University (LSU), students of Professor D. Larry Crumbly, CPA, Cr.FA, CFFA, FCPA, have compiled a series of papers that address these characteristics as part of their studies in Forensic Accounting.

In Lisa Eversole’s paper, “Profile of a Fraudster,” “egotistical, risk taker, rule breaker, under stress, financial need and pressured to perform” were among the characteristics identified. In a review of criminally prosecuted health care fraud cases, these same conditions similarly were mentioned. She went on to observe: “The gains from the fraud can be direct (receipt of money or property) or indirect (reward or promotions, bonuses, power or influence).”<sup>6</sup> In the next section, a system to classify these behaviors will be introduced.

## The Hierarchy of Greed

Maslow’s Hierarchy of Need is often represented as a pyramid, with physiological needs at the bottom and self-actualization at the top. In researching this topic, five levels of greed have been used to similarly classify health care’s “Hierarchy of Greed<sup>sm</sup>.”<sup>7</sup> Using a pyramid, these five types of greed are: undisciplined, opportunistic, corporate, scheme and organized. A definition and discussion of each follows.

**Undisciplined Greed** – is typified by an individual(s) whose inquisitive mind(s) lead them to “sneak a peek” at celebrity medical records – more out of curiosity than for profit; but nonetheless, a serious breach of medical data security.

**Opportunistic Greed** – adds an “opportunity” factor to undisciplined greed and parlays it into a motive by selling

that information for personal gain. This category also includes individuals who commit fraud against insurance companies.

**Corporate Greed** – raises the bar from the staff levels usually found in undisciplined and opportunistic greed, and involves organizational leadership. The notion of “loophole exploitation” is introduced to see how much of a factor it plays when corporate greed is examined in the context of not-for-profit vs. for profit entities.

**Scheme Greed** – The very sound of the word connotes evil wrongdoing, and is most often exemplified by an outright plan to steal information to profit by its use in defrauding governmental insurance plans.

**Organized Greed** – Yes, it can involve organized crime; but more often provides an expansive base from which schemes are hatched, expanded from within a familial circle, and copycatted by others looking to profit from ill gotten gains.

When taken together, these five factors cover a wide-range of health care fraud and abuse. While not necessarily a perfect classification system, it allows for type casting the bad actors that have been disciplined, fined, or incarcerated; and provides some insight into the factors that influenced these bad behaviors. As a result, some additional safeguards can be considered. These discussions follow.

### Crimes and Punishment

“Don’t do the crime, if you can’t do the time!”<sup>8</sup> In cases of health care fraud and abuse, penalties can range from payment restitution to criminal incarceration. In instances in which internal hospital medical records are breached, punishment ranges from reprimands to dismissal, with civil and criminal proceedings possibly based upon the extent of the infraction, and consequential damages caused by the actions.

### The EMR isn’t Facebook

“Friend me, tweets, and text messaging” have become commonplace; but all too often that commonplace activity also occurs in the workplace. After a recent mass transit accident in Boston, a trolley driver admitted to “texting while operating the vehicle” while rear-ending another trolley in front of it.<sup>9</sup> While the case will no doubt look to place future sanctions and prohibitions on carrying and using cell phones, personal digital assistants (PDAs) and the like by transit employees, you need only look around any hospital setting (or for that matter, any office setting) to see this common occurrence.

Surprisingly, after reading two Internet postings (there are probably more), the health care industry will need to brace for the impact of “Twitter Surgery – In the Operating Room,”<sup>10</sup> and the “4 Things You Shouldn’t Do While Texting” including circumcision and surgery),<sup>11</sup> which may portend an even greater risk than celebrity data breaches.

The sanctity of the medical record, whether the traditional hard-copy variety, or the newer electronic medical record (EMR) that is

dotting the landscape in ever increasing numbers, is vulnerable to the “sneak a peak,” also known as celebrity data breaches. “Our society’s insatiable desire to know everything about celebrities, especially the private details of their lives, has reached a new low with recent news out of Los Angeles. Also at a new low here: patient confidentiality. The UCLA Medical Center is moving to fire 13 employees and disciplining 12 others, for peaking at the confidential patient history of pop star Britney Spears, the Los Angeles Times reports.”<sup>12</sup>

These are not isolated events, although they may have a geographic locus on the East and West coasts. “When a famous Hollywood actor is suddenly admitted to your hospital, some employees will likely be tempted to take a peek at the heartthrob’s medical records. But when the hospital in question later suspends more than two dozen employees without pay for allegedly violating privacy rules, those involved are bound to question whether ‘the punishment fits the crime,’ and to what extent the hospital could have better protected its celebrity patient.”<sup>13</sup>

These instances of “undisciplined” behavior may be rooted in celebrity viewing, but in another episode at UCLA Medical Center in which celebrity breaches of such notables as Farrah Fawcett and California’s First Lady, Maria Shriver, have occurred, the same individual who viewed Fawcett’s records, also viewed 61 other patient records—including those of noncelebrities.<sup>14</sup> While undisciplined actions seem to attract attention and notoriety associated with celebrities, the impact tends to be localized, as long as the data breach is contained and not exploited for profit and gain, as shown in the next section.

### Identity Crisis

Whether watching television or surfing online, the airwaves and cyberspace are filled with offers and advertisements to check your credit report, and prevent financial identity theft. Far less evident in the literature, and almost certainly absent from the media glare is the matter of medical identity theft. Though the two types of theft are rooted in the same premise that something personal has been stolen, the extent of the impact, the detection timeframe and the consequences and prevention techniques are in need of tightening in the health care industry.

The “undisciplined” persona noted above turns greedier when it becomes “opportunistic,” and it is no longer a voyeuristic event, but one where data is stolen and sold. For example, while medical data breaches at UCLA Medical Center were discussed above, an employee at the same facility pleaded guilty to selling patient medical information to tabloid publications in 2007.<sup>15</sup>

While tabloids are one avenue to entice the opportunistic individual, another more sinister plot unfolds when staff with access to data can be compromised to sell patient information to unknown third parties. In the incident involving New York-Presbyterian Hospital/Weill Cornell Medical Center, a staff member was arrested for selling data to persons who approached the individual offering money for information. The reported payments of \$750 and \$600 for at least two sets of 1,000 patient

data files seems small compared to the risk of losing one's job and likely facing criminal prosecution. The potential damage resulting from the misuse of this data, however, could cause financial and medical identity theft affecting very large patient populations.<sup>16</sup>

Financial identity theft seeks to impersonate an individual by accessing their credit cards, bank accounts and personal data. Medical identity theft, while borrowing some of the same key demographics that make up one's "protected health information," results when another individual improperly poses as the patient, or one's insurance identification is improperly used. These errant entries in the medical record may go undetected for long periods of time and become difficult to correct.

"Medical identity theft is a crime that can cause great harm to its victims. It also is the most difficult to fix after the fact because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years."<sup>17</sup> Medical identity theft is caused in large part by the type of schemes that involve theft of patient and physician information resulting in billing fraud that will be discussed in more detail. Because of its striking similarity to financial identity theft, however, these two problem areas are grouped together and classified as opportunistic greed.

While a good portion of the undisciplined and opportunistic health care fraud is associated within the framework of organizational entities, individuals commit health care fraud against their own insurance companies. This may take the form of submitting personal claims that are false or erroneous. In instances in which these individuals are caught, their defenses range from ignorance to everyone is doing it, to the insurance company won't miss a few dollars."<sup>18</sup> Prosecutors often cite nongovernmental health insurers in having better systems and resources to detect and prevent claim fraud than do the federal government's Medicare and Medicaid programs.

### "Someone Always Playing Corporation Games"<sup>19</sup>

"Corporate Greed" is listed third on the hierarchy of greed. In the first two categories: undisciplined and opportunistic, the individual tends to be a staffer and not a department head or executive. In corporate greed, we start the climb that may take us into the "C-suite." The perplexing question is why?

Many "not-for-profit" organizations find themselves with large settlements, corporate integrity agreements, and in some cases incarceration for fraudulent acts. On the surface, it may appear more obvious that in the "for profit" health care sector there might be more corporate greed, given higher salaries, bonuses, and stock options that serve as the motivating factors. Those successful in the not-for-profit sector, however, often use their accomplishments as a springboard to the more lucrative for profit sector. Then again, the increasing levels of executive compensation in the not-for-profit sector have risen to such heights that congressional investigations have taken a closer look, especially as the voluntary not-for-profit organizations struggle to deliver services and meet the community benefit needs during increasingly difficult reimbursement and regulatory periods.

With these conditions as a backdrop, three other factors warrant consideration as possible precursors to criminal activities: ego, misguided altruism, and loophole exploitation.

(1) **Ego** – Bragging rights may have something to do with this.

Hospitals are ranked in national publications, and even have mortality and other measures becoming commonplace on state health department websites. Additionally, in "Profit of a Fraudster," Eversole said "the perpetrator may be scornful of obvious control flaws...and beating the organization [or system] is a challenge and not a matter of economic gain alone."<sup>20</sup>

(2) **Misguided Altruism** – By most accounts, hospitals nationwide have been operating on razor thin margins – with those in New York State (NYS) often on no margin at all. This makes the case of the seven NYS hospitals named in a \$50 million lawsuit alleging kickbacks, billing for unnecessary services, and providing treatment without a license,<sup>21</sup> a possible case of misguided altruism gone badly. Interestingly, in another article it was reported that "No criminal actions are alleged in the complaint. But the attorney general had harsh words for those named in the complaint."<sup>22</sup>

(3) **Loophole Exploitation** – In a good many instances, the use of civil remedies tend to be applied to what is here termed, "loophole exploitation." While it may be called "gaming the system" or "pushing the envelope," cases for erroneous billing whether associated with outliers, diagnosis-related group (DRG) code assignment, cost reporting, kickback, or various types of billing therapies, these cases generate considerable negative publicity, and often result in steep fines and penalties being levied.

While inexcusable in the eyes of the law, the motives behind these vehicles seem more rooted in misguided altruism, rather than the egregious behavior that is discussed in the next two behavioral levels of greed. Although the types of corporate greed discussed above were centered in the hospital and health system and physician arenas, corporate greed has new frontiers in the pharmaceutical and pharmacy segments, with many cases being brought both civilly and criminally.

Some prosecutors see less behavioral causation, and instead believe its economic risk that weighs as a more significant contributing factor. They emphasize that it is the choices that management often makes in deciding in favor of one project or another determines whether management evaluates economic gains vs. risks. Citing more recent examples of hospital settings vs. pharmaceuticals, they conclude that "pharma" has become more "risk aware and risk averse" after years of being penalized significantly and substantially. Additionally, there has been more restraint as a result of having the overall number of companies reduced in size, and specifically because the companies' boards will directly hire and fire the chief executive officers. In contrast, hospitals and health systems will (still) get it wrong when competing projects pit the general good of the hospital vs. the good of individual and competing departments. Too often, the "actors" don't have the full frame of reference and incomplete knowledge from which to make objective and legally correct recommendations.

### When Strategies Becomes Schemes

The literature talks about "schemes," particularly as they relate to those individual(s) who steal Medicare and Medicaid identification

numbers and unique physician identification numbers to bill fraudulently. The most prominent schemes are found today in the Durable Medical Equipment (DME) and infusion therapy services.

Surprisingly, many of these crimes are perpetrated by individuals or small groups of people often related to each other. In dissecting the backgrounds of these schemes, prosecutors report that ethnicity and barriers to workforce entry of those in lower socio-economic rankings make for a recipe to enter criminal enterprises. So rampant has this phenomenon become that federal task forces have been formed in an all-out effort to dismantle these illegal activities and prosecute the guilty parties. Medicare is a trust-based system, and prosecutors have found over the years that schemers have found ways to take advantage of its thinly reinforced protective barriers. Now with this all-out effort to add manpower and data and analytic prowess, prosecutors hope to derail these current schemes; although they are wary that further vulnerabilities are simply one schemer away from starting over again.

### The Sopranos Meet Health Care

At the top of the Hierarchy of Greed pyramid is “organized greed.” “Health care fraud is not just committed by dishonest health care providers. So enticing an invitation is our nation’s ever-growing pool of health care money that in certain areas - Florida, for example - law enforcement agencies and health insurers have witnessed in recent years the migration of some criminals from illegal drug trafficking into the safer and far more lucrative business of perpetrating fraud schemes against Medicare, Medicaid, and private health insurance companies.”<sup>23</sup>

It may not be too difficult to see how the opportunistic behavior associated with financial and medical identity theft, and the individual scheming characterized by ethnicity and lower economic standing has led to organized crime seeking a foothold in health care fraud. Pam Dixon, Executive Director, World Privacy Forum, said: “...there have been cases involving Russian organized crime and identity theft rings that are buying health clinics and billing the government for services.”<sup>24</sup>

While it’s been noted that organized crime may find health care fraud less likely to be detected, and that its penalties less harsh, a review of more recent convictions and penalties suggests otherwise. The joint strike forces that are now operating in Miami and Los Angeles bring all of the power of the federal government to bear. This is particularly noticeable when the convictions appear on the Internal Revenue Services web site where penalties appear to increase exponentially for the added charges of tax evasion and money laundering. When mail fraud also is evident, penalties also increase. The government is trying to combat the problem with an increasingly large arsenal of weapons at its disposal.

### Conclusion

Part I of this article has examined those who have committed fraud and the characteristics that may have led to their criminal behavior. It also has defined varying degrees of greed, as behavioral traits common to the criminal mind. Part II will examine the way many compliance structures work to detect and prevent

fraudulent activities, sophisticated data models used to guard against identify theft and record breaches, the screening of new hires and the reevaluation of existing staff to see if lapses exist that threaten to exploit vulnerable areas, and related perspectives and vantage points to address compliance concerns. ■

*Allan P. DeKaye is President and Chief Executive Officer of DEKAYE Consulting, Inc. His firm assists health care clients with financial, compliance and operational issues. He is a frequent speaker at national conferences, and is author/editor of The Patient Accounts Management Handbook (Aspen). Mr. DeKaye also is a member of the CCH Health Care Compliance Editorial Advisory Board. For more information: call: (516) 678-2754; write: dkconsult1@aol.com, or visit: www.dekaye.com*

- <sup>1</sup> Maslow, A., *Motivation and Personality*, (1954).
- <sup>2</sup> Simons, J.A., Irwin, D.B., Drinnien, B. A., *Psychology – The Search for Understanding*, West Publishing Company, New York, 1987, as excerpted in: Maslow’s Hierarchy of Needs, found at: <http://honolulu.hawaii.edu/intranet/committees/FacDevCom/guidebk/teachtip/maslow.htm> at 1.
- <sup>3</sup> Boeree, Dr. C. George, Abraham Maslow, 1908-1970 (Biography) at 2, found on: <http://webspace.ship.edu/cgboer/maslow.html>.
- <sup>4</sup> “Abraham Maslow’s Hierarchy of Needs Theory,” as discussed at: [http://www.envisionsoftware.com/Management/Maslow\\_Needs\\_Hierarchy.html](http://www.envisionsoftware.com/Management/Maslow_Needs_Hierarchy.html).
- <sup>5</sup> “Maslow’s Hierarchy of Needs,” as discussed at: <http://www.businessballs.com/maslow.htm> at 8.
- <sup>6</sup> Eversole, L., “Profile of a Fraudster,” as presented at: <http://www.bus.lsu.edu/accounting/faculty/lcrumbley/fraudster.html> at 1.
- <sup>7</sup> Healthcare’s “Hierarchy of Greed<sup>sm</sup>” is a service mark of DEKAYE Consulting, Inc.
- <sup>8</sup> Lyric from: “Baretta’s Theme Keep You Eye on the Sparrow.” Words and Music by: Morgan Ames and Dave Grusin.
- <sup>9</sup> Valencia, M.J. and Bierman, N., “MBTA: Conductor in Boston trolley crash was texting his girlfriend,” Boston Globe, May 8, 2009.
- <sup>10</sup> Found at: <http://stanford.wellsphere.com/healthcare-industry-policy-article/twitter-surgery-in-the-oper...>
- <sup>11</sup> Found at: <http://southcoasttoday.com/apps/pbcs.dll/article?AID=/20090514/SC2470105/90513> (Jason Perry, southcoast247.com, assistant editor).
- <sup>12</sup> “Celebrity Medical Records Accessed Without Authorization,” April 8, 2008 at 1, as reported at: <http://identitytheft911.org/alerts/alert.ext?sp=10439>.
- <sup>13</sup> “HIPAA Compliance Strategies: Alleged Breach of George Clooney’s Health Information Leads to Suspension of 27 Staffers at NJ. Medical Center,” published at: [http://www.aishealth.com/Compliance/Hipaa/RPP\\_Geroge\\_Clooney\\_PHI.html](http://www.aishealth.com/Compliance/Hipaa/RPP_Geroge_Clooney_PHI.html).
- <sup>14</sup> *Supra* n. 12 at 1-2.
- <sup>15</sup> “Former Hospital Employee Gave National Enquirer Celebrity Medical Records,” as presented at: <http://www.hulig.com/2623/73906/former-hospital-employee-gave-national-enquirer-celebr...>
- <sup>16</sup> “NYC Hospital Worker Charged with Stealing Patient Info,” as presented at: [http://www.1010wins.com/print\\_page.php?contentID=1873268&contentType=4](http://www.1010wins.com/print_page.php?contentID=1873268&contentType=4).
- <sup>17</sup> Dixon, P., “Medical Identity Theft: The Information Crime that Can Kill You,” The World Privacy Forum, May 3, 2006, at 5.
- <sup>18</sup> “Who Commits/Reports Healthcare Fraud,” available at: [http://www.deltadentalnj.com/fraud/who\\_commits\\_fraud.shtml](http://www.deltadentalnj.com/fraud/who_commits_fraud.shtml).
- <sup>19</sup> Lyric from “We Built This City,” Jefferson Starship. Words and Music by: Bernie Taupin, Martin Page, Dennis Lambert and Peter Wolf.
- <sup>20</sup> *Supra* n. 6 at 2.
- <sup>21</sup> Mason, J., “Hospital Accused of Medicaid Fraud,” The Daily Mail, Jan. 5, 2009, available at: <http://webmail.aol.com/4291/aol/en-us/mail/PrintMessage.aspx>.
- <sup>22</sup> Minissale, J., “Cuomo sues CMH for fraud,” Indenews.com, Jan. 1, 2009, available at: [http://www.midhudsoncentral.com/site/printerFriendly.cfm?brd=248&dept\\_id=462341&n...](http://www.midhudsoncentral.com/site/printerFriendly.cfm?brd=248&dept_id=462341&n...)
- <sup>23</sup> “The Problem of Health Care Fraud,” National Health Care Anti-Fraud Association, at 3., available at: [http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti\\_fraud\\_resource\\_center&wpsc](http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_center&wpsc).
- <sup>24</sup> McKay, J., “Identity Theft Steaks Millions from Government Health Programs,” Feb. 13, 2008, at 2., available at: [http://www.govtech.com/gt/print\\_article.php?id=260202](http://www.govtech.com/gt/print_article.php?id=260202).

©2009 CCH. All Rights Reserved. Reprinted with permission from the Health Care Compliance Letter

# Inside Criminal Minds, Part II

by Allan P. DeKaye, MBA, FHFMA

*Part I of Inside Criminal Minds discussed individuals who have committed fraud, and the characteristics that may have led to their criminal behavior. It also defined the varying degrees of greed, as behavioral traits common to the criminal mind.*

Part II of the article examines: (1) the way many compliance structures work to detect and prevent fraudulent activities to see if it provides sufficient safeguards, (2) the more sophisticated data models used to guard against identify theft and record breaches, (3) the way we screen new hires and re-evaluate existing staff to see if lapses or loopholes exist that threaten to exploit vulnerable areas, and (4) related perspectives and vantage points to address compliance concerns.

## Detection, Deterrents, Safeguards and Cultural Retooling

Prosecutors contend that regardless of the reason, bad actors, whether in health care or other industries, need to be brought to justice. While the hierarchy of greed seeks to provide some level of classification and insight into those who become these bad actors, it also may provide the industry with some additional ways to detect and deter fraud, waste and abuse from occurring in the first place. In this section, some of these approaches will be presented, along with a discussion of other factors conveyed by those with different vantage points.

### The Cost of Drilling

For most hospitals, health systems and health care corporate entities, compliance plans and training seem to be the first line of defense against fraud, waste and abuse. But how effective are these programs? This author's own experience in providing training and education suggests that compliance topics are presented, but that retention of fact and practical application often falls short of obtaining a passing grade.

While stuck in traffic, I had a recollection of my military days (many years ago); however, I was able to recite closely (but not verbatim), the U.S. Army's three General Orders: (1) "I will guard everything within the limits of my post and quit my post only when properly relieved; (2) I will obey my special orders and perform all of my duties in a military manner; and (3) I will report violations of my special orders, emergencies, and anything covered in my instructions to the commander of the relief."<sup>25</sup>

Sound familiar? With a few substitutions, it could read like a standard compliance plan. Why could this subject content be recalled almost some 40 years after first hearing it? Perhaps the answer lies in the same way we remember the Multiplication (Times) Tables. Drilling! Whether in the public school

systems, or in Basic Training at Fort Campbell, Kentucky.

In attempting to curtail or limit the urge or need for the undisciplined level of greed, the sneak-a-peak mentality, health care providers will need to "drill" the core precepts of corporate compliance training into staff with the same military precision and warning: that your life depends on it – or in today's terms – your job depends on it! The cost of such repetitive and frequent training, however, is high. Revisiting the training curriculum to ensure that even shorter, more frequent reminders of core principles (whether in classroom, staff meetings, newsletters, or online vehicles, etc.) would be more beneficial than simple annual compliance retraining sessions that may be embedded in other organizational training (e.g., fire safety, etc.).

### Finding and Training Better Actors

In discussing this and other training phenomenon with Ken Kruger, President and CEO, Healthcare Human Resources Consulting Consortium, LLC (White Plains, New York), he cited that pre-hiring competency and behavioral assessment as being important measures health care organizations should use in hiring, especially for deterring the "opportunistic level of greed." He went on to add that leadership skills assessments are now being introduced with more frequency. He said that these assessments helped organizations find team players, good decision-makers, and spokespeople.

Kruger also indicated that behavioral interviewing gave management a better indication of how an individual would handle work related situations. Criminal background checks and drug-testing were becoming more prevalent in health care, and that these steps would help deter and prevent corporate greed.

He spoke favorably of employee assistance programs, but also noted that in large organizations, you find employee's personal issues are often associated with bad behavior. From his own vantage point in Human Resources leadership and consulting, he found activities like loan-sharking and drug problems were to be found. He noted that the use of cameras not only helped guard against patient care issues, and facility perimeter security, but often led to detection of criminal activity, arrests, and prosecutions.

Prosecutors confirmed that in the medical arena, arrests for corporate greed and schemes were often linked to personal problems, whether financial, marital or drug-related, to mention a few. They also indicated that individuals may be subjected

to fear of losing their job in situations in which supervisory or leadership personnel pressures staff into committing fraudulent activities as they act out corporate greed. While this ties back to Maslow's need for safety and (job) security, the effectiveness of compliance training (and drilling) should prevent employees from being victimized. Understanding their "duty to report" is essential to combating internal and external threats.

### CSI: Health Care

In mounting its counterattack on health care fraud and abuse, the federal government is marshalling its resources from across all of its criminal fighting divisions. One tool that it is using with great success is data mining. By analyzing vast amounts of claim data, federal task forces in Miami and Los Angeles have been able to tackle schemes and organized greed in DME and infusion therapy fraudulent billing activities.

Health care providers also are using advanced data mining to find internal areas of weakness and potential for abuse. While many systems may send an alert if an unauthorized individual is attempting to gain access to a medical record, other organizations are going further.

In some instances, health care systems track the usage of those individuals who have legitimate business reasons for accessing patients' accounts and medical records. They have added different algorithms and tracking protocols to compare volumes and patterns of usage an individual may have. For example, an Admitting Registrar ordinarily might have reason to access 100 patient records a day to perform his or her assigned tasks; however, the safeguards detect when "150" or "500" records are accessed in timeframes outside of the norm. Department heads then receive these reports, and must satisfactorily explain these variances in very short time frames. These types of protocols can provide a line of defense to prevent undisciplined and opportunistic greed from occurring or progressing to more serious situations.

### Raising the Red Flag

The health care industry was included in the Federal Trade Commission's (FTCs) "Red Flag" rules designed to combat identity theft. While the types of advanced data mining protocols described above can help health care organizations prevent and detect internal and external influences, the red flag approach helps organizations guard against patient perpetrated fraud. The rules also can help organizations shore up their data defenses from weaknesses caused from within.

Although some health care organizations have wrestled with designing and implementing such a policy and procedure, it would seem important to consider several of the following approaches to assure that the patient being treated is who he or she claims to be.

(1) **Requesting a Driver's License** – A seemingly benign request for a driver's license is often met with resistance. The Joint Commission (Joint Commission on the Ac-

creditation of Healthcare Organizations) requires that two forms of identification (ID) be provided (one of which is a picture ID) to promote patient safety. The driver's license (or a state issued nondriver's license), passport, or other form of government or picture identification provides vital demographic data necessary to retrieve the patient's medical record on subsequent visits or admissions, as well as to permit proper billing to insurance companies.

- (2) **Obtaining the Social Security Number (SSN)** – Obtaining the SSN perhaps may be more difficult and of concern given the level of identity theft that occurs. Many hospital information systems, however, use the SSN as a record key to more easily retrieve a patient's medical record when returning for subsequent care. All too often, failure to obtain the SSN results in that specific data field being filled with the ubiquitous "000-00-0000" or "999-99-9999," depending on the choice of default value. As a result, patients with the same name, as well as those with similar names sounding the same, hospitals have a universal problem with the same patient registered more than once with duplicate medical record numbers.
- (3) **Duplicate Medical Records** – Duplicate medical records by their very nature should prompt a "red flag" warning. They prevent clinicians from obtaining a complete medical history and provide a pathway for the undisciplined, opportunistic, or schemer to find a reservoir of personal and financial information for purposes of medical identity theft that may go undetected and unreported.
- (4) **Credit Scoring and Data** – Credit scoring and data is controversial, but is being used by some facilities nonetheless. Similar to the authority (the FTC) that indicates that health care providers are covered by red flag rules, the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA) indicates that because health care providers extend credit, they have "permissible purpose" to use credit data and reporting. It can be a helpful indicator to access, in addition to patient provided information, other factors that may support an application for financial assistance, charity care or Medicaid. This type of data also can provide fraud alerts such as: the person is deceased, the SSN was never issued, or the SSN was issued to someone who is deceased, etc. Credit files also contain aliases, previous addresses, and access to other data sources that can help establish and confirm identity.
- Health care organizations are reticent about using credit scoring and data, and often cite the Health Insurance Portability and Accountability Act (HIPAA) concerns for not using some or all of this data. This seemingly selective invocation of HIPAA suggests that if a facility cannot safeguard patients' financial information (e.g., credit file data), then how capable is it in safeguarding patients' medical data, and other protected health information. Failure to protect either leaves health care providers vulnerable to the various forms of greed described throughout this article.

### **“To err is human, to forgive divine”<sup>26</sup>**

There'll be no forgiveness in health care fraud – the federal government is turning up the HEAT. In a May 20, 2009 press release, the new administration's Attorney General and HHS Secretary announced the formation of a new interagency effort, the “Health Care Fraud Prevention and Enforcement Action Team (HEAT).” HEAT will expand the Medicaid Fraud Strike Forces now in operation in South Florida and Los Angeles to Detroit and Houston.<sup>27</sup>

While the schemes and organized greed will be in the HEAT crosshairs, health care provider organizations will need to do more to protect themselves from corporate greed. Gregory J. Naclerio, Esq., health law partner at Ruskin Moscou Faltischek, PC (Uniondale, New York) and Co-Chair of the firm's White Collar Crime and Investigations Group, used the “misguided altruism” case of the seven New York State Hospitals noted above to remind hospital executives and boards of trustees, “that even if their best intentions were to serve the needs of the community and hospital their due diligence needs to peel back the multiple layers of contracts to detect possible violations.” Naclerio, himself a former Director of the Long Island Regional Office of the Deputy Attorney General for Medicaid Fraud Control, indicated that greed often starts out small, and then grows. He cited that boards of trustees had to become more engaged in the process of safeguarding their institutions to better fulfill their fiduciary responsibility.

In describing the increased responsibility trustees of health care organizations have, Jeffrey Blumengold, FHFMA, CPA, partner and practice leader, Healthcare Services Group, WithumSmith+Brown, PC, indicated that, “New Jersey hospital Trustees are now required to complete a formal Trustee Training program, which must be approved by the Health Commissioner and is believed in the view of the state to be necessary for Trustees to ‘keep pace with best practices for governance, monitoring of quality and efficiency and financial oversight,’ and which should help those governing hospitals in that state to become more aware of their responsibilities and also the complex conditions which can lead to fraud, waste and abuse.” Blumengold, whose firm provides health care organizations with a full-range of audit, tax, and consulting services in the New Jersey, New York, and Pennsylvania region, notes that regulations often aren't simply black and white and that federal and state regulations, at times, are at odds with one another. He suggests that this “grey matter factor” can be a contributing element to the conditions typically present for fraud or abuse to occur. Moreover, while Professional Accounting Standards require that audit teams “brainstorm,” looking for ways fraud may be committed during the audit planning process that is conducted prior to a health care audit, he cautions that in the end, “Pressure/Incentive,” “Opportunity,” and “Rationalization” are essential ingredients in completing the fraud triangle. Thus, having both management and its trustees ever vigilant, on the lookout for questionable behavior or actions, is essential in serving to deter, detect, and ultimately prevent fraud.

While Congress is likely to continue its pressure on hospital providers through a more focused look at executive compensation, intended more to ensure that these facilities meet their community benefit obligations, the corporate greed that continues to be found

in the for profit sector may require forensic accountants to consider how the timing of financial statements may mask more alarming greed. In a paper, “Is There a Relationship Between Management Compensation and Revenue Management,” the authors suggest studies have been inconclusive in drawing a connection between management compensation and misstatements of revenue. They conclude that instead of measuring compensation variables during or at the end of a misstatement period, they examine the time period immediately prior to the beginning of the misstatement period. “This technique ensures that our measures reflect whether compensation may have led to misstatement, rather than capturing how the misstatement itself may have affected the compensation.”<sup>28</sup>

In a case of life imitating art, “Earnings Management: The Game,” describes a game that was developed to identify corporate dishonesty. It's used as part of a Master of Accountancy program, and is based on this precept: “Forensic accountants must identify environmental variables that encourage or inhibit management dishonesty. This paper describes a game used to help students understand that information asymmetry exists between managers and the public, and that public information may be misstated to increase management wealth.”<sup>29</sup>

The game creates a series of outcomes associated with dealing cards and rolling dice to determine if the students (read managers) need to reveal earlier predictions about the cards and dice truthfully. Perhaps the introduction of these types of games into the hiring process, at board presentations or conference calls with stock analysts would have a sobering impact: to tell the truth.

## **What Were They Thinking?**

### **Five Headlines for Five Levels of Greed**

“Another Day, Another Celebrity's Hospital Record Breached”<sup>30</sup> (Undisciplined Greed); “Reports: Hacker Demands \$10 Million for Records”<sup>31</sup> (Opportunistic Greed); “FL Health System Settles Medicare Fraud Charges”<sup>32</sup> (Corporate Greed); “Three People Indicated for Defrauding Medicare Through Billing Scheme...”<sup>33</sup> (Scheme Greed); “Does Healthcare Fraud Tie into Organized Crime, Illegal Immigration and...Corporations?”<sup>34</sup> (Organized Greed).

There were certainly more headlines from which to choose, and there may well be more than the five levels of greed as defined in this article. But the question that should keep gnawing at us – is why?

Perhaps opportunistic greed could be explained in part by a conclusion of the Association of Certified Fraud Examiners (ACFE), when ACFE President, James Ratley, noted: “The message to Corporate America is simple – desperate people do desperate things. Loyal employees have bills to pay and families to feed. In a good economy, they would never think of committing fraud against their employers.”<sup>35</sup> This is reminiscent of Maslow's need for safety and security gone awfully wrong.

The comments by Byron Hollis, Esq., CFE, AFHI, however, seem to draw a different conclusion, “Health care fraud has been with us for as long as we have had health-care insurance programs. Fraud is driven by a basic human weakness. We are all tempted by greed and we all are intrigued by the idea of getting something for

nothing. Unfortunately, some people succumb to the temptation at the expense of others.”<sup>36</sup> This thinking would support the notion that greed can occur in any of the five levels.

Another popular belief is that scheme and organized greed are advanced by career criminals and organized crime groups. “In the North Carolina Medicare case, three subjects residing in North Carolina traveled to Florida where relatives taught them how to anonymously file false Medicare claims. They returned to North Carolina and began filing such claims. Unless people in your state don’t have any connections to people in other states, chances are, somebody is using a sophisticated scam that they learned elsewhere.”<sup>37</sup> Prosecutors will concur with this premise calling health care fraud: “regional and viral.”

### Bad Actors, Bad Plays

“The plays the thing wherein I’ll catch the conscience of the King.”<sup>38</sup> Prosecutors talk about “bad actors” as the culprits in health care fraud. They also cite the inherent weaknesses in the Medicare and Medicaid systems (“the plays”) that leave them vulnerable to attack. That leaves “conscience” as the remaining variable that can influence the outcome of events.

Lest we forget, the False Claims Act has its origins dating back to the Civil War. Perhaps it is inherent human characteristics that shape and define bad behavior that is not only found in health care, but in other industries, too. Recognizing that behavioral traits, economic concerns and opportunities may be “triggers” of the hierarchy of greed, then remedies and preventive actions can be tailored to limit the rash of fraud, abuse and waste that exists today.

If it were only that simple that we could treat celebrity data breach or identity theft with a dose of penicillin, we might be issuing a prophylactic dose to those in high risk areas. The examples of those losing their jobs, or facing stiff monetary penalties or incarceration may finally begin having a deterrent effect to limit recurrence. More involved and educated boards using stronger data-mining, and other protective layers and more effective training may further insulate organizations from corporate greed. New legislation pending in Florida, which will soon require DME and other type entities to post bonds (proposed to be about \$500,000) before obtaining their provider numbers is expected to cut down on the fly-by-night billing frauds that are found in scheme and organized greed. Even federal audits of the Medicare and Medicaid program point out that government contractors need to tighten and improve their review and payment processes to close those areas of vulnerability.

We hear a lot today about auto insurers offering “accident forgiveness,” and that good drivers won’t have their premiums raised if they have an accident. Given the level of audits, ranging from Recovery Audit Contractors (RACs) to state Office of the Medicaid Inspector General (OMIG), perhaps organizations that consistently pass these audits with stellar outcomes should be given this same dispensation either from future audits or an easement in the event of some accidental (not fraudulent) occurrence. We should consider that for good actors, there should be something other than the absence of a penalty.

With the prospect that health care reform legislation might be enacted sometime in the near future, we could hope to expect stron-

ger internal and external controls. New regulations may help pave the way for it. There are, however, often unintended consequences that can emanate from legislation and regulation. Nationally, many jurisdictions have installed red-light cameras to promote intersection safety. While the number of red-light runners are reported down (and revenues up for violators), there has been concern with the number of rear-end collisions increasing in these situations. Behavioral changes need to occur, and training and re-education over time will be needed to fully realize the expected benefits.

If the hierarchy of greed can help explain in some way what is inside criminal minds, then it is possible that the remedy lies in the precision of the laser beam (e.g., task forces, data mining, and education, etc.) being trained and focused on the diseased portions of the brain (e.g., levels of greed) to remove the various lesions. It would be ironic to conclude that the scalpel might be mightier than the sword.

*Allan P. DeKaye is President and Chief Executive Officer of DEKAYE Consulting, Inc. His firm assists health care clients with financial, compliance and operational issues. He is a frequent speaker at national conferences, and is author/editor of The Patient Accounts Management Handbook (Aspen). He is a member of the CCH Health Care Compliance Editorial Advisory Board.*

<sup>25</sup> Army General Orders (For Boot Camp), presented at: <http://usmilitary.about.com/od/armyjoin/1/blbasicgenorder.htm>.

<sup>26</sup> Pope, A., “An Essay on Criticism.”

<sup>27</sup> HHS News Release, Attorney General Holder and HHS Secretary Sebelius Announce New Interagency Health Care Fraud Prevention and Enforcement Action Team,” May 20, 2009, available at: <http://www.hhs.gov/news/presw/2009pres/05/20090520a.html>.

<sup>28</sup> Du, H., Cullinan, C.P., and Wright, G.B., “Is There a Relationship Between Management Compensation and Revenue Misstatements,” *Journal of Forensic Accounting (Article Abstract)*, Vol. VIII (2007) at 119.

<sup>29</sup> Lovata, L.M., Earnings Management: The Game,” *Journal of Forensic Accounting (Article Abstract)* Vol. VIII (2007) at 227.

<sup>30</sup> Headline in: Security, Privacy and The Law, April 4, 2009, available at: <http://www.securityprivacyandthelaw.com/2009/04/articles/medical-information/another-day...>

<sup>31</sup> Headline in: Health Data Management, May 6, 2009, available at: [http://www.healthdatamanagement.com/news/breach-28169-1.html?type=printer\\_friendly](http://www.healthdatamanagement.com/news/breach-28169-1.html?type=printer_friendly).

<sup>32</sup> Headline in Fierce Healthcare, Dec. 19, 2006, available at: <http://www.fiercehealthcare.com/node/4505/print>.

<sup>33</sup> FBI Press Release: (Los Angeles Division), May 24, 2007, available at: <http://losangeles.fbi.gov/pressrel/la052407.htm>.

<sup>34</sup> Headline at: Blogger News Network, Feb. 14, 2008, available at: <http://www.bloggernews.net/113782>.

<sup>35</sup> Kostigan, T., “When going gets tough, the help embezzles,” *MarketWatch*, May 29, 2009, available at: <http://www.marketwatch.com/story/story/print?guid=B7ECC957-371F-407F-95EA-4N98E>.

<sup>36</sup> “Health-care fraud drains lifeblood from patients, systems,” *Fraud Magazine*, March/April 2006, at 2, available at <http://www.acfe.com/fraud/view-content.asp?ArticleID=542>.

<sup>37</sup> Mathias, R., “Health Care Fraud Schemes Committed by Career Criminals,” *Mathias Consulting*, April 10, 2003, presented at: <http://mathiasconsulting.com/node/79/print>.

<sup>38</sup> Shakespeare, W., *Hamlet*, Act 2, scene 2, 603-605.