

CCH Healthcare Compliance LETTER

Volume 6, Issue 4

www.cchgroup.com

March 3, 2003

On The Front Lines

Fearing a revolution: Genetics and the Privacy Rule (part I of II)
by Gordon R. Shea, J.D.

HIPAA

- Final HIPAA Security Rule ready

Fraud & Abuse

- Excluded MD gets x-ray software company position
- Relevant conduct key to Anti-kickback sentencing

False Claims

- Government may *Swiftly* decline fraud case; *Sequoia* cut down

Letters to the Editor

The CCH Healthcare Compliance team welcomes comments regarding articles published in the CCH Healthcare Compliance Letter. Send comments to Jeff Reinholtz, Managing Editor at reinholj@cch.com. For more information about the CCH Healthcare Compliance Portfolio visit our online store at <http://health.cch.com>.

Final HIPAA Security Rule ready

by Gordon R. Shea, J.D.

The Department of Health and Human Services (HHS) announced the long-awaited administrative Final Security Rule component of the Health Insurance Portability and Accountability Act (HIPAA). Most entities subject to the Rule will have until April 21, 2005 to comply; small health plans will have an additional year.

Flexibility. The newly finalized Security Rule mandates physical, administrative, and technical safeguards to protect healthcare data. The *sine qua non* of the Rule is elasticity. In a Tuesday, February 18th audio conference conducted by the organizers of the HIPAA Summits and hipaaudioconferences.com, HHS Advisor Karen Trudel told listeners that the government “erred on the side of flexibility” in developing the new Rule’s standards. The government has emphasized that two of the organizing principles they used in developing the Rule ensure that the Rule was not associated with specific technologies and that the Rule could be effectively implemented by HIPAA “covered entities” (a term of art defined elsewhere in the law) of all types. The ultimate Final Rule, HHS said in accompanying commentary, was written “as generic as possible” so that the standards it announced “may be met through various approaches or technologies.”

One example of the Rule’s flexibility is found in the issue of data backups. According to the Federal Register, one individual who submitted comments on the proposed Rule raised concerns with how the Rule might impose data backup standards. HHS responded by saying that data backups “should be stored in a secure location with controlled access. The appropriate secure location and access control will vary, based on the security needs of the covered entity.” For example, the agency said, a simple lock-and-key storage area may be best for one entity whereas another entity might be required to store data backups at a secure off-site facility that specializes in electronic data protection. Both procedures would satisfy the Security Rule’s provisions on data backups.

One of the most substantial parts of the Final Rule is a standard for administrative safeguards (as enumerated at §164.308 of the Rule). This standard would require covered entities to take what HHS has called “appropriate” steps to safeguard their data and perhaps just as importantly, periodically update those safeguards and document their efforts.

Narrows the scope. The Rule, promulgation of which was required by Title II(f), §§ 261-264 of HIPAA, was originally proposed in 1998 and was, at that time, kept open for public feedback. According to information released by HHS, the agency received and considered approximately 2,350 comments on its proposals before finalizing the Rule.

The now final Rule differs from its initially-proposed text primarily in that it narrows the scope of information that will be subject to new security standards. Under the Rule as first proposed, essentially **all** electronic health information that pertained to individuals would have been subjected to the Security Rule. By contrast and under the most current version, only **protected** health information kept in electronic form would be subject to the Final Rule. In another major departure from the first-proposed Rule, the Final Security Rule contains no standard for electronic signatures although such a standard will likely be promulgated in the future. While the proposed Rule mandated various “requirements” and “features,” the final version instead mandates “standards” and “implementation specifications.”

In addition, the Rule now requires that HIPAA “covered entities,” engaged in the sending or maintenance of electronic information, to assess their potential vulnerabilities as well as other risks and that they develop, implement, and maintain appropriate measures to safeguard that information. In commentary accompanying the announcement of the Rule, HHS emphasized that this duty will be ongoing and will evolve rather than being a requirement that can be met with a one-time-only review process.

According to commentary released just in advance of the Final Rule, the new standards in the Rule are based on widely accepted security principles, standards that already exist throughout the industry. These standards are based on recommendations that were made several years ago by the National Research Council and advice from healthcare security experts.

Privacy & training. In another much-watched area and in the run up to finalization of the Rule, HHS has made clear that the Security Rule is closely linked with HIPAA’s Privacy Rule. To some extent, this linkage was expected and obvious, since confidential healthcare information clearly

must be kept secure in order to remain private. In the most obvious practical example of this type of linkage between the two Rules, the final Security Rule now plainly states that it shares the definitions of most key HIPAA concepts – such as “business associate” and “health information” – with those definitions set forth in the Privacy Rule.

The government has emphasized, however, that there are some important distinctions between the Security and Privacy rules. While the Privacy Rule essentially deals with issues of *control* over information – how infor-

The Rule mandates physical, administrative, and technical safeguards; the government ‘erred on the side of flexibility’ in developing its new standards.

mation is used, when it may be disclosed, and what rights healthcare patients may have in terms of information being revealed – the Security Rule speaks to physical, administrative, and technical matters as means of protecting the integrity and availability and not *only* the privacy of information. In terms of scope, the Privacy Rule governs health information in all forms while the narrower Security Rule applies only to information that is kept electronically.

Another important part of the final Security Rule is training. During the HIPAA Summit/hipaaudioconferences.com teleconference on Tuesday, February 18th, for example, presenter John Parmigiani, Director of HIPAA Compliance Services with CTG HealthCare Solutions, Inc., called the final Security Rule “people-focused.” The final rule will require “reasonable and appropriate” workforce training. These requirements have been

grouped under a single standard in the Final Rule, at §164.308. While HHS disagreed with commentators who wished all of the Security Rule’s training provisions to be issued as guidelines rather than requirements, HHS has emphasized that they will remain flexible in terms of the amounts and types of training required.

HHS’s commentary on the Final Security Rule is available at <http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049fecon-ofr-2-12-03.pdf>. ■
Final Rule, 68 FR 8334, Feb. 20, 2002, ¶100,919



Managing Editor
Jeff Reinholtz, J.D.

Coordinating Editors
Raio G. Krishnayya, J.D.
Gordon R. Shea, J.D.
Geraldine S. Stroka, J.D., R.N.
Judith A. Tichenor, J.D., L.C.S.W.

CCH Washington Bureau
HHS, CMS–Brendan Frost
DOJ, FTC–Peter Feltman
Capitol Hill–Catherine Hubbard,
Jeff Carlson

White House–Paula Cruickshank

Designer
Tom O’Connor

Comments from readers are welcome and should be directed to Jeff Reinholtz at REINHOLJ@CCH.COM, Tel. 847-267-7316, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Healthcare Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is \$305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO CCH Healthcare Compliance Letter, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A. All rights reserved. ©2003 CCH INCORPORATED.

No claim is made to original government works; however, the gathering, compilation, and arrangement of such materials, the historical, statutory and other notes and references, as well as commentary and materials in this Product or Publication are subject to CCH’s copyright.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Unless otherwise noted, all paragraph references are to the CCH Healthcare Compliance Reporter.

Excluded MD gets x-ray software company position

by Geraldine S. Stroka, J. D., R.N.

Individuals excluded from federal healthcare programs have limited job opportunities at companies receiving federal funding because the potential for secondary liability upon the employer that receives the federal funding is great since the law generally prohibits recipients of federal monies from allowing excluded providers from rendering services in exchange for federal funding. Thus, corporations may be leery about hiring excluded providers without official approval from oversight and enforcement agencies like the Office of Inspector General (OIG). One software company, which sought such approval, received the green light from the OIG.

The Office of Inspector General (OIG) permitted the software company to hire an excluded physician because, according to the company, the physician would not be: (1) furnishing services or items reimbursable by any federal healthcare program, and (2) associated with the division of the company furnishing such items or services. This begs the question about why the software company sought to hire such a physician.

Business development position.

The software company (which also provided data services) developed a product designed to digitize and store x-ray images. The sole market for that product was healthcare facilities and providers reimbursed by federal healthcare programs. The physician was sought out by the software company to assist the company in enhancing its business development programs for marketing its products to healthcare entities. The software company made it clear, however, that the position for which the physician was being sought required no contact with patients or healthcare providers involved in federal healthcare programs.

Exclusion-related laws. Generally, there are numerous reasons for excluding a provider from participation in federally funded healthcare programs. Some of those reasons can be found in the Soc. Sec. Act §1128 (b)(4), (CCH Healthcare Compliance

Reporter ¶16,457B). The Act prohibits payment for any item or service furnished by an excluded person. Civil monetary penalties can be imposed on any person or entity that employs or contracts with excluded individuals for items or services payable by federal healthcare programs.

The laws and regulations are very clear; a provider or entity receiving federal healthcare funding in very limited situations may employ excluded individuals.

Federal healthcare program payment will not be made for items or services furnished, directly or indirectly, by an excluded individual, irrespective of who actually submits the bills. These prohibitions extend to employment or contracts with an excluded individual or entity even if the excluded individual or entity: (1) is paid with non-federal funds, (2) is paid by an unrelated third party, or (3) provided the items or services free of charge.

Sufficiently separable. The laws and regulations are very clear; a provider or entity receiving federal healthcare funding in very limited situations may employ excluded individuals. These situations would include instances where payment is made exclusively from private funds or from other non-federal sources. Another situation where a federally funded provider may employ an excluded individual occurs where the excluded person provides services only to nonfederal programs or patients.

In this case, the company represented that the physician would not be furnishing any items or services reimbursable, directly or indirectly, by any federal healthcare program, and associated with the division producing the x-ray computer software product. Based on those representations, the OIG determined that the purpose and funding of the physician's position were so weakly connected to any federal healthcare program that his/her hiring would not violate the physician's exclusion and would, therefore, not incur any sanctions. ■

OIG Advisory Opinion 03-01, Jan. 21, 2003, ¶150,198

continued on page 6

CCH Healthcare Compliance Editorial Advisory Board

Timothy P. Blanchard, Esq.
McDermott, Will & Emery

Neil B. Caesar, Esq.
President
The Health Law Center

Paris Cavic, J.D., MBA
The Healthcare Compliance Group, L.L.C.

Bill Dacey, MBA, MHA, CPC
President, The Dacey Group

Allan P. DeKaye, MBA, FHFMA
DeKaye Consulting, Inc.

Louis H. Feuerstein
Partner, HIPAA Privacy Series
Ernst & Young

Michael A. Murer, J.D.
Murer Consultants, Inc.

Elizabeth O'Kelly, Esq.
Former Corporate Compliance Officer
Northwestern Memorial Hospital

Cynthia F. Reaves, Esq.
Honigman Miller Schwartz and Cohn

Theodore J. Sanford, Jr., M.D.
Chief Compliance Officer for
Professional Billing
University of Michigan Health System

William P. Schurgin, Esq.
Seyfarth, Shaw, Fairweather & Geraldson

Jackie Selby, Esq.
Vice President and Health Care Counsel
Oxford Health Plans, Inc.

Nancy L. Shalowitz, MHA, J.D.
Director for Health Law & Graduate Programs
DePaul University College of Law

John E. Steiner, Jr., Esq.
Chief Compliance Officer for
Cleveland Clinic Health System

Sanford V. Teplitzky, Esq.
Ober, Kaler, Grimes & Shriver

L. Stephan Vincze, J.D., LL.M., CHC
Ethics & Compliance Officer
TAP Pharmaceutical Products, Inc.

Fearing a revolution: Genetics and the Privacy Rule (part I of II)

by Gordon R. Shea, J.D.

A law protecting the privacy of genetic information has long been the Holy Grail of healthcare privacy advocates. There are some indications that the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule may serve as such a law now or in the future. Yet one of the few fields of American life that has already seen genetics-based privacy issues play out is the workplace. What is happening on that field shows a disconnect between courts and policymakers.

"We wish to learn philosophy by rote, and play at heroism. But the wiser God says, Take the shame, the poverty, and the penal solitude, that belong to truth-speaking. Try the rough water as well as the smooth. Rough water can teach lessons worth knowing.... Fear not a revolution, which will constrain you to live five years in one. Don't be so tender at making an enemy now and then."

—Ralph Waldo Emerson

Introduction. The Office of Civil Rights (OCR) within the Department of Health and Human Services (HHS) recently put guidance on its website flatly stating that "genetic information is health information protected by the Privacy Rule."

This does not necessarily make it so. First, so-called "Guidance" posted on an OCR web page is hardly likely to be considered mandatory legal authority whenever the first case involving HIPAA and genetics is litigated. Second, a close reading of the next sentence on the OCR web page statement muddies the issue. After stating that "Yes, genetic information is health information protected by the Privacy Rule," the OCR Guidance goes on to add: "Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse." This suggests that genetic information is not *per se* protected; instead, it is protected only if it meets a certain legal definition — a definition that may be narrower than it seems. While the first prong of that definition seems easily met (genetic material by its very nature will virtually always be individually identifiable) the second prong has more loopholes than might be initially obvious.

The most immediate battleground for these issues has been the workplace. This is because employers have a particular interest in trying to identify the genetic predispositions and "weaknesses" of prospective and current employees. It is also evidenced by the fact that the employment context is one of the few places where there is anecdotal evidence that genetic-based discrimination has already occurred. In addition, the employ-

ment context has given rise to the few cases of alleged genetic discrimination such as *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, (discussed further *infra*) which have resulted in a real vetting by the judicial system (as opposed to out-of-court settlements and the like). The workplace setting provides a prime example of the kind of complexities that OCR's guidance does not even begin to address. Most employers are not "covered health care providers, health plans, or health care clearinghouses" under HIPAA. Yet many employers who do not fall under such HIPAA definitions are still interested in screening employees for certain genetic information.

Background. Whether or not privacy-invasive workplace genetic testing is even enough of an issue for the law to address is still open for debate. A 2001 survey by the American Management Association (AMA) reported that genetic testing by employers "remains extremely rare." Only two of the companies the AMA surveyed reported engaging in such testing of workers or prospective workers. Nevertheless, at least one commentator has plausibly noted that concerns about genetic testing in the workplace date back to at least the 1970s. During that era, "many leaders in the Black community felt that sickle cell anemia was not receiving adequate medical attention." In response, "Congress passed the National Sickle Cell Anemia Control Act of 1972 to appropriate federal funds for voluntary testing programs." Around the same time, however, "some scientists suggested that" carriers of the sickle-cell gene might be uniquely susceptible to certain chemicals common in many workplaces. Problems in the hiring and retention of sickle-cell-positive workers resulted along with obvious related issues of confidentiality. In addition, the same AMA survey that deemed genetic testing "rare" in the modern workplace still found that 68% of surveyed companies reported engaging in some type of workplace medical testing.

Furthermore, one recent report by a group of healthcare privacy advocates cites study and survey evidence suggesting that the general public is concerned about the privacy of their genetic information. There is also the fact that just because there have been few ongoing controversies about the privacy

of genetic information to date, does not mean that there will not be in the future, or that genetic privacy is somehow unworthy of being addressed by the legal system. Equal Employment Opportunity Commission member Paul Miller recently expressed “concern” that “if employers are permitted to consider genetic information in making personnel decisions, people may be unfairly barred or removed from employment for reasons that are wholly unrelated to their ability to perform their jobs.” The “potential for genetic discrimination is real,” according to Miller, “and no longer just the stuff of science fiction.”

HIPAA itself. Regardless of how one takes the OCR’s recent issuance of website “guidance” flatly stating that “genetic information is health information protected by the Privacy Rule,” HIPAA unquestionably does address the issue of genetics to some extent. In fact, HIPAA is the first federal law debated and passed by both houses of Congress and signed by the President to explicitly address genetic discrimination in any way. Section 701 of the HIPAA statute’s text states that health insurers “may...impose a preexisting condition exclusion” on insureds “only if...such exclusion relates to a condition (whether physical or mental), regardless of the cause of the condition, for which medical advice, diagnosis, care, or treatment was recommended or received within the 6-month period ending on the” insurance enrollment date. Shortly thereafter, the text says that “Genetic information shall not be treated as” such “a condition [i.e., a preexisting condition]...in the absence of a diagnosis of the condition related to such information.” What is notable about this is the focus on diagnoses. Even if a person’s DNA suggests, in the strongest possible way, that the person is predisposed to develop a certain illness, insurers cannot hold that against the person unless and until a formal medical diagnosis of that illness has been rendered. This has been called a “significant change in the law.” Section 701 is, however, confined to purely insurance aspects of HIPAA, and does not address the *privacy* of genetic information.

Other legal protections. In the absence of completely clear and specific Privacy Rule protection for genetic information other attempts to protect genetic privacy have been undertaken in a piecemeal fashion. In February 2000, then-President Clinton signed executive order 13145 “to prohibit discrimination against employees based on protected genetic information, or information about a request for the receipt of genetic services;” so-called “protected genetic information” singled out by the Order include information about an individual’s, or an individual’s family’s, genetic tests. Being an executive order, however, this law was not subject to debate in Congress; hence, the truth of the earlier remark that HIPAA is the first federal law debated and passed by both houses of Congress and signed by the President that explicitly addresses genetic discrimination.

Creative plaintiff’s lawyers have also done a good job of stretching existing laws to try and shoehorn genetic privacy protections into existing legal frameworks. Probably the best example of this

is the U.S. Court of Appeals for the Ninth Circuit case of *Norman-Bloodsaw v. Lawrence Berkeley Lab*. The question presented in *Norman-Bloodsaw* was “whether a clerical or administrative worker who undergoes a general employee health examination may, without his knowledge, be tested for highly private and sensitive medical and genetic information such as syphilis, sickle cell trait, and pregnancy.” The plaintiffs in the case were “current and former administrative and clerical employees of” the defendant laboratory, which is “a research facility operated by the...Regents of the University of California pursuant to a contract with the” federal Department of Energy (DOE). As described by the Ninth Circuit, the DOE requires all federal contracting laboratories

[T]o establish an occupational medical program. Since 1981, it has required its contractors to perform ‘preplacement examinations’ of employees as part of this program, and until 1995, it also required its contractors to offer their employees the option of subsequent ‘periodic health examinations.’ The mandatory preplacement examination occurs after the offer of employment but prior to the assumption of job duties. The Department actively oversees Lawrence’s occupational health program, and, prior to 1992, specifically required syphilis testing as part of the preplacement examination.

Most of the plaintiffs in *Norman-Bloodsaw* had

[R]eceived written offers of employment expressly conditioned upon a ‘medical examination,’ ‘medical approval,’ or ‘health evaluation.’ All accepted these offers and underwent preplacement medical exams. Two of the plaintiffs also were subjected to additional examinations. The examinations included questionnaires about the plaintiffs’ medical history including questions about “whether the patient had ever had any of sixty-one medical conditions, including ‘sickle cell anemia,’ ‘venereal disease,’ and, in the case of women, ‘menstrual disorders.’” Urine and blood samples were also taken as part of the examinations. All employee samples “were tested for syphilis; in addition, certain samples were tested for sickle cell trait; and certain samples were tested for pregnancy.

Part II of this series will examine the outcome of the *Norman-Bloodsaw* case, compare how that outcome relates to the Privacy Rule, and consider the implications for the privacy of genetic information.

Gordon R. Shea is a licensed attorney and a CCH Healthcare Compliance Law Analyst and Editor. Several of his HIPAA writings are collected on the website www.hipaa.chh.com. For more information, Mr. Shea may be contacted at CCH INCORPORATED, 2700 Lake Cook Road, Riverwoods, Illinois 60015, Phone: (847) 267-2812, E-mail: sheag@cch.com.

On The Front Lines

Continued from page 5

- ¹ <http://www.emersoncentral.com/culture.htm>
- ² <http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf>
- ³ See, e.g., Bryce A. Lenox, COMMENT: GENETIC DISCRIMINATION IN INSURANCE AND EMPLOYMENT: SPOILED FRUITS OF THE HUMAN GENOME PROJECT 23 *Dayton L. Rev.* 189, 190, n. 2 (Fall, 1997) (reporting on a “twenty-four-year-old social worker” who “received several promotions and excellent performance reviews over an eight month period, but was fired after her employer learned that she was at risk for Huntington’s Disease...”) See also **Marisa Anne Pagnattaro**, *GENETIC DISCRIMINATION AND THE WORKPLACE: EMPLOYEE’S RIGHT TO PRIVACY V. EMPLOYER’S [sic] NEED TO KNOW*, 39 *Am. Bus. L.J.* 139, Fall, 2001 (reporting that “during a job interview, a fifty-

three-year-old man disclosed that he was diagnosed with asymptomatic hemochromatosis. In his second interview, he was told that the company was interested in hiring him, but would not be able to offer him medical insurance; during a third interview he was told that “although they would like to hire him, they were unable to do so because of his hemochromatosis.”) Pagnattaro also reports on *Burlington Northern Santa Fe Railroad and Mayfield v. Dalton*, two cases about employers who wished to engage in genetic testing of employees. Neither case made it beyond initial procedural stages in the courts.

- ⁴ <http://www.amanet.org/research/archives.htm>
- ⁵ *Id.*
- ⁶ **Pagnattaro**, supra note iii.
- ⁷ *Id.*
- ⁸ *Id.*
- ⁹ *Id.*
- ¹⁰ <http://www.amanet.org/research/archives.htm>
- ¹¹ *Genetics and Privacy*, ihealthreports, prepared

by the Health Privacy Project, April, 2002 <http://www.chcf.org/topics/view.cfm?itemID=19759>.

- ¹² ARTICLE: DISCRIMINATION IN EMPLOYMENT ON THE BASIS OF GENETICS: PROCEEDINGS OF THE 2002 ANNUAL MEETING, ASSOCIATION OF AMERICAN LAW SCHOOLS SECTION ON EMPLOYMENT DISCRIMINATION LAW, 6 *Empl. Rts. & Employ. Pol’y J.* 57 National Employee Rights Institute & Chicago-Kent College of Law
- ¹³ *Id.*
- ¹⁴ <http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf>
- ¹⁵ Pagnattaro, supra note iii, at 166.
- ¹⁶ Exec. Order No. 13145, 65 *Fed. Reg.* 6877 (Feb. 8, 2000).
- ¹⁷ *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 9th Cir. Ct. of Appeals, (1998).
- ¹⁸ *Id.* at 1264.
- ¹⁹ *Id.*
- ²⁰ *Id.* at 1265.

Fraud & Abuse (cont.)

Relevant conduct key to Anti-kickback sentencing

by **Raio G. Krishnaya, J.D.**

The Anti-kickback statute operates such that as a practical matter, a violation usually involves at least two or more parties. This fact gives rise to the potential for not only a charge under the predicate offense, but also allows the government to attach a conspiracy count. Also, the potential for upward departures can be significant depending upon how intertwined a defendant’s involvement was in the conspiracy. A recent U.S. Court of Appeals for the Tenth Circuit case, *U.S. v. McClatchey*, addresses precisely this issue and illustrates how courts may handle the issue.

History. The Tenth Circuit opinion is the latest in the *McClatchey* line of cases that has addressed many issues pertaining to the Anti-kickback Statute. The *McClatchey* history began in 1985 when Baptist Medical Center entered into an agreement with two physicians, Robert and Ronald LaHue, principals of the Blue Valley Medical Group. At that time, McClatchey was the Chief Operating Of-

ficer (COO) for Baptist. The terms of the agreement stated that the LaHues were to be appointed as “Co-Directors of Gerontology Services” for Baptist in exchange for a fee of \$75,000 per LaHue, per year. Shortly thereafter, the LaHues began referring patients that required hospital care to Baptist.

The agreement technically expired in 1986; however, Baptist continued to pay the LaHues and the LaHues continued to refer patients, thus creating a contract by implication. In 1991 Baptist had been planning to merge with Health Midwest. The Baptist attorney, Mark Thompson, assigned to conduct the due diligence review, noted that no contract existed to memorialize the agreement between the LaHues and Baptist. Thompson also realized that the execution of the implied contract was opening up Baptist to Anti-kickback statute liability. Thus, Thompson sought a method to craft a contract to bring the LaHue-Baptist arrangement within a safe harbor. However, this required negotiation with the LaHues to reach an agreement on terms that would accomplish Thompson’s goal. McClatchey became the key player in those negotiations.

Two years later, a contract was finally drafted and the LaHues solidified the con-

tinued flow of revenue in exchange for patient referrals with Baptist. However, the negotiations became fodder for securing McClatchey’s conviction, because those negotiations demonstrated that McClatchey **knew** that the LaHues were not performing the services required under the contract as indicated by Baptist employees. In addition, McClatchey learned from some of the same employees that Baptist had no interest in the LaHues services. Lastly, the negotiations stressed the underlying fiscal importance to Baptist of having the LaHues’ referrals.

Interestingly, McClatchey’s conviction became a legal football. The jury that heard McClatchey’s case found him guilty of conspiracy to violate the Anti-kickback statute as well as guilty of the predicate offense. His defense counsel sought to have the jury’s verdict set aside and in a somewhat unusual move, the trial court did just that, concluding there was, “insufficient evidence from which a reasonable jury could find McClatchey had a specific intent to violate the Act.”

Eventually McClatchey’s conviction was reinstated, the trial court, using the United States Sentencing Guidelines (USSG), calculated McClatchey’s offense level as eight. The court then granted a

three level downward departure, which resulted in a sentence of three years probation with six months of electronically monitored home detention. The government appealed, resulting in this latest decision in this case's history.

Sentencing calculus. Understanding sentencing calculations under the USSG can be somewhat daunting as it can be confusing. This latest opinion in the *McClatchey* history provides a thorough analysis of how a sentence may be imposed under the Anti-kickback statute, as well as considering the complex calculus that comes into play when a conspiracy conviction must also be factored in.

The court began its analysis by noting that an Anti-kickback violation starts as a level eight under the USSG under the "Bribery in Procurement of Bank Loan and Other Commercial Bribery" section of the USSG. Interestingly, since the time of McClatchey's original sentencing and the appeal, the USSG was amended to include an upward departure table, which did not exist at the time McClatchey was sentenced. Therefore, McClatchey's sentence was to be calculated pursuant to the unamended version of the USSG.

From the initial level of eight, the crux of the appeal materialized because under the USSG the amount alleged in the scheme dictates the degree of increase in a departure from the initial level. Thus, under McClatchey's view, his involvement amounted to \$50,000, substantiating at most a five level upward departure. The trial court agreed with McClatchey. The government, however, disputed this \$50,000 figure and was significantly disparate in its calculation of the amount involved, \$1.2 million. The basis for the government's number was that the \$1.2 million was the amount involved in the conspiracy to which McClatchey was an integral part, thus making him culpable for the entire amount in the conspiracy.

The USSG notes that a defendant, who has "jointly undertaken criminal activity (a criminal plan, scheme, endeavor, or enterprise undertaken by the defendant in concert with others, whether or not charged as a conspiracy), could be liable for "all reasonably foreseeable acts and

omissions of others in furtherance of the jointly undertaken criminal activity." Thus, the question is for what reasonably foreseeable conduct is McClatchey liable?

The court noted that this was an issue of fact in that the scope of McClatchey's conduct would dictate what would constitute relevant conduct. While the Tenth Circuit agreed that although McClatchey could be responsible for some conduct under the conspiracy, he could not be responsible for all conduct occurring under the conspiracy. Recall that McClatchey's conviction was for involvement in the post-1986 contract, thus legal impossibility would preclude McClatchey from being liable for more than the post-1986 contract. Thus, the calculation by the trial court included a formula in which the amount at issue was the difference between the bribe paid minus payments to the LaHues that were legitimate. Therefore, the trial court concluded that the bribe paid to the LaHues amounted to \$150,000 but that the LaHues performed \$100,000 in legitimate services, which placed McClatchey in liability for \$50,000 to which the Tenth Circuit agreed.

Downward departure. Most practitioners are aware that a significant factor in sentencing is the inclusion of mitigating circumstances. Such circumstances, if accepted under the USSG, can result in substantial downward departures. In McClatchey's case, he asserted three mitigating factors: (1) extraordinary family circumstances, (2) aberrant behavior, and (3) a combination of the two factors.

The Tenth Circuit noted that family circumstances are not normally recognized under the USSG as statutory mitigators. However, courts are allowed latitude to consider such factors if the circumstances are "present to an exceptional degree or in some other way makes the case different from the ordinary case where the factor is present."

The circumstance forwarded by McClatchey was the need to care for his son who suffered from severe psychological disabilities. McClatchey argued that the severe nature of his son's disabilities required him to constantly monitor his son's health, as well as to maintain consistency in his treatment.

The court, however, did not accept this as a factor that rose to the level previously articulated for several reasons. First, the court noted that while McClatchey's son's need for care was intensive, the record did not support a finding that **only** McClatchey could conduct this level of care. Regardless of McClatchey's assertion that transferring this burden to other family members was untenable, the court found that such a downward departure would be impossible under the USSG. Siding with precedence, the court noted that the disruptive nature and the difficulties imposed on those related to the defendant are "inherent in the punishment of incarceration."

As to the issue of "aberrant behavior", McClatchey's argument was that this conduct was out of the ordinary and that such conduct would otherwise have a very low probability of occurrence. Again, the court, considering the "totality of the circumstances," disarmed this argument for downward departure. McClatchey's attempt to persuade the court that his conduct fell under the aberrant behavior standard included proffers of his education and employment history, his superb behavior while on bond, his cooperative behavior during investigation and throughout the proceedings, and his community service. Each of these factors was disallowed under the Tenth Circuit's consideration of the aberrant behavior factor. On the contrary, the court noted that many of these characteristics would strongly support an argument that McClatchey should have known better.

Conclusion. The *McClatchey* court concluded by imposing a sentencing level of 13, reversing the original level of eight under the USSG. *McClatchey* reinforces the lesson that the concept of "reasonably foreseeable" can be somewhat ambiguous in that different courts impose, to a greater or lesser degree, responsibility upon defendants for the conduct of their co-conspirators. Furthermore, it is a reminder that challenging a conspiracy charge is not only limited to the culpability phase of a case, but also plays a determinative role in sentencing. ■

U.S. v. McClatchey, No. 01-3327, 10th Cir., Jan. 16, 2003, ¶102,041

Government may Swift-ly decline fraud case; Sequoia cut down

by Gordon R. Shea, J.D.

A recent ruling by the United States Court of Appeals for the District of Columbia (D.C.) — one that runs counter to the decisions of at least one other major court — allows the government virtually unfettered discretion to beg off *qui tam* False Claims Act (FCA) cases, regardless of the wishes of the relator.

DOJ concedes accusation. While the case *Swift v. U.S.* (which at press time was still subject to pre-publication revision) was from a non-medical context and involved issues of seemingly frivolous litigation, the D.C. appellate court's decision broadly addresses the right of the government to remove itself from, and altogether decline, relator-initiated FCA litigation. The case might ordinarily be of little interest but for the fact that it bluntly questions a legal test announced not long ago by the U.S. Court of Appeals for the Ninth Circuit in the case of *U.S. ex rel. Sequoia Orange Co. v. Baird-Neece Packing Corp.*, 151 F.3d 1139 (9th Cir. 1998).

Swift began when a former Department of Justice (DOJ) employee named Susan Swift filed a *qui tam* action against two fellow employees. The DOJ conceded Swift's main allegation, which was that the two employees had defrauded the federal government out of about \$6,200 by falsifying leave slips and time sheets. However, the government refused to intervene in the case and moved to dismiss it, saying that the case was too expensive to pursue given the modest amount of money involved. Swift argued that the government's move was wrong on both procedural and substantive grounds. Procedurally, she maintained, the government could not move to dismiss without first intervening; substantively, Swift claimed that the government's stated position about dis-

missing the litigation based on its expense was a mere pretext against getting involved in a case that it preferred to bury.

Substantive: executive discretion.

Under *Sequoia*, the government may dismiss a *qui tam* case over the relator's objection only when the government (1) shows that the dismissal is rationally related to a valid purpose, and (2) can refute any legitimate relator allegations that the decision to seek dismissal was arbitrary, capricious, fraudulent, or illegal.

The *Sequoia* test, the D.C. Court of Appeals said, raises constitutional separation-of-powers questions because it "authoriz[es] judicial review of the government reasons" for dismissing FCA cases. The *Sequoia* court justified that outcome on the basis that it did not unduly burden the exercise of executive branch discretion in bringing or joining cases. Writing for the D.C. Court of Appeals, however, Judge Randolph called that justification "not an accurate statement of constitutional law with respect to the government's judgement not to prosecute."

"The Constitution entrusts the Executive with the duty to 'take Care that the Laws be faithfully executed,'" Judge Randolph noted. "The decision whether to bring an action on behalf of the United States is therefore 'a decision generally committed to [the government's] absolute'" discretion. There is no language in the FCA, the Judge continued, that "purports to deprive the Executive Branch of its historical prerogative to decide which cases should go forward in the name of the United States." Turning to specific provisions of the FCA that require relators to be granted hearings when they want them prior to dismissal of FCA litigation, the D.C. court concluded "that the function of a hearing when the relator requests one is simply to give the relator a formal opportunity to convince the government not to end the case."

While the Ninth Circuit grounded its *Sequoia* test in part on some legislative history behind a 1986 amendment to the FCA, the D.C. appellate court indicated that the Circuit was far off base in doing so. The relevant legislative history, Judge Rudolph wrote, "relates to an unenacted Senate version of the 1986 amendment." Rudolph added that even if the court were to use the *Sequoia* test in the *Swift* case, "the government easily satisfied" it. "The asserted governmental interests were that the dollar amount was not large enough to warrant expending resources.... While [Susan Swift] asserted that the government's reasons for dismissal were pretextual, she offered nothing to support the charge."

Procedural: "largely academic" As to plaintiff Swift's procedural arguments, the D.C. Court of Appeals noted that 31 U.S.C. §3730(c)(1), one part of the FCA, states that when the government decides to proceed with an FCA action, the relator still has the right to continue as a party in the case, "subject to the limitations set forth at" §3730(b)(2). In turn, it gives the government 60 days to elect to intervene and proceed with FCA actions that have been brought to its attention. In plaintiff Swift's view, subsections (c)(1) and (b)(2) were so closely interrelated that the government could never move to dismiss an FCA case unless it had first intervened and proceeded with the litigation to some extent.

"Nothing in §3730(c)(1) justifies that reading," Judge Randolph wrote for the court. "In any event," he continued, the question of whether the FCA requires the government to intervene before dismissal is "largely academic," because even "if there were such a requirement, we could construe the government's motion to dismiss as including a motion to intervene," and dispose of the case that way. ■

Swift v. U.S., D.D.C., No. 01-5312, Feb. 11, 2003, ¶1305264

HIPAA Privacy Training

When you're ready to implement your company's HIPAA compliance training, look to CCH's **HIPAA Privacy Training** to prepare your employees. **HIPAA Privacy Training** provides case study scenarios plus feedback explaining each correct answer to the true/false and multiple choice questions. Additionally, **HIPAA Privacy Training** aids supervisors by offering an Administrator's Guide with answer key, plus test record forms for auditing purposes as well as individualized certificates of completion for each trainee.