Journal
OF GOVERNMENT FINANCIAL MANAGEMENT® FALL 2017 VOL. 66, NO. 3

Protecting Governments' Data

AGA®

Ethics and Protecting Government Data

By: Melinda DeCorte, CGFM, CPA; and Diane MaKaeli, MPA

Government employees are in unique positions that provide them with access to private, confidential and protected information. When our positions give us access to information the general public does not have, it is imperative we use and disclose this information only as authorized, and for approved business purposes. Citizens have a right to privacy; their personal and confidential information — obtained by, stored within, and shared among our profession — must be kept secure.

When our knowledge is gained as a result of access to privileged information, professional ethics requires we maintain confidentiality, and securely protect this information. With ongoing exposure to confidential information within the scope of our jobs, we must not become complacent or take for granted the seriousness of protecting this data. We cannot use it for self-serving purposes or disclose it, either of our own volition or by persuasion, without proper authorization.

For example, work in the health-care field often requires daily access to private health information. It is common for this information to be utilized over the course of the workday. But what if your supervisor, after seeing emergency responders at his neighbor's house, wanted to know what type of treatment was provided? Or, what if a celebrity received care, and you thought sharing specifics would liven a party? How would you handle the pressure to share this information? What if you are just personally curious and want to view private information on someone you know or know of, even if you do not intend to do anything more with the information? Is it ethical? As accountability professionals, we must never take advantage of the privileges our positions afford, including access to non-public information. Furthermore, we are required to prevent inappropriate access to, and disclosure of, personal and confidential information.

Any private, confidential or privileged information made known to us in a professional capacity — adhering to disclosure standards — must be protected and secured. Every state has its own law imposing an obligation to protect the confidentiality of patient health information, and there are federal requirements established in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and expanded under the HIPAA Omnibus Rule, in 2013.

Prior to the use, access or disclosure of patient information, it must be confirmed that authorization from the patient or their legal representative has been received, and the information falls within the permitted purposes. The patient also has a right to know who has accessed or been provided their information. It is essential that proper recordkeeping policies and procedures are in place that track access to and disclosures of information that requires authorization prior to release.

Education, policies and procedures, which conform to the rules and regulations, are in place to ensure the protection of this data. Inappropriate access to protected information can not only harm the victim, but also negatively affect our profession. It is important we hold ourselves and our profession to the highest ethical standards.

Recall the news stories about the U.S. Department of State employees who snooped through the passport files of three presidential candidates — Senators Barack Obama, Hillary Clinton and John McCain — and the inspector-general investigation that followed. Although this was nearly 10 years ago, the embarrassment these incidents caused the department likely lingers.

When applying for or renewing a passport, citizens have an expectation that data — including name, gender, Social Security number, photograph, and date and place of birth — provided during the application process, and stored in an electronic system, will be

Two easy ways to submit an ethics question:

1. EMAIL:
journal_ethics@agacgfm.org

2. ONLINE:
www.agacgfm.org/journal_ethics

protected. In some cases, additional evidence needed to review and adjudicate the application, such as citizenship and criminal records, is also maintained in the passport file with the application. This information is protected under The Privacy Act of 1974 (Privacy Act). Access to this system is limited to authorized Department of State employees and contractors who need access to perform their official duties.

In addition to the protection of this information under the Privacy Act, federal employees are bound by standards of ethical conduct that include not engaging in financial transactions using nonpublic government information or allowing the improper use of such information to further any private interest.[1]

Although the purpose of the system is to provide authorized users the ability to query information on previously processed passport applications in the performance of their official duties, it is possible to imagine the curiosity a user might have in querying passport applications of celebrities, politicians and other high-profile individuals. The Department of State's inspector general investigated such activities based on the claims that the files of these three presidential candidates had been breached. The investigation showed passport files of more than 120 famous individuals had been accessed repeatedly, and it was not evident that access was required in the conduct of official duties. The report cited "control weaknesses, including a general lack of policies, procedures, guidance and training," as reasons for the unauthorized access.[2] Furthermore, it is clear these individuals were not adhering to ethical standards, using nonpublic government information to further a private interest.

As shown through these examples and likely seen in your own experiences, government accountability professionals have a responsibility to protect and appropriately use the confidential information to which they have access. If the information is misused, it not only violates our professional ethics, but can also lead to job termination and possible criminal charges.

AGA's *Code of Ethics* specifically sets forth a fundamental principle of confidentiality — "do not disclose or use any confidential information acquired during the course of performing professional services."[3] In adhering to our code of ethics, AGA members and CGFMs are expected to do the right thing in any given situation. And we, and fellow members of the AGA Professional Ethics Board, are here to help.

Endnotes

1. 5 C.F.R. Part 2635: *Standards of Ethical Conduct for Employees of the Executive Branch*. www.gpo.gov/fdsys/pkg/CFR-2011-title5-vol3/pdf/CFR-2011-title5-vol3-part2635.pdf; accessed June 14, 2017.
2. U.S. Department of State and the Broadcasting Board of Governors Office of Inspector General, Office of Audits AUD/IP-08-29 July 2008. www.hsdl.org/?view&did=235939; accessed June 14, 2017.
3. www.agacgfm.org/codeofethics; accessed June 14, 2017.

Melinda DeCorte, CGFM, CPA, president of AGA's Dallas Chapter, is also vice chair of AGA's Professional Ethics Board.

Diane MaKaeli, MPA, is CEO of Global Business & Financial Services. She is the education chair and immediate past president for AGA's Seattle Chapter, and serves on AGA's Professional Ethics Board.