Volume 6, Issue 1

Compliance Matters

A Publication from the Office of Compliance and Risk Management

In This Issue:

Clearing Conflicts of Interest on the Path to Professional Enhancement

When as administrators we seek to strengthen and advance our professional portfolio by engaging in professional or business activities outside of our jobs at NYU we may unknowingly be stepping over potential conflicts of interest. Does the outside consulting work we may be doing in addition to our NYU job, the personal outside business we may have set up, the part-time employment for another employer, the board membership at a for-profit or non-profit create a potential conflict of interest with our job responsibilities at NYU? These are threshold questions we may not have stopped to ask. This article focuses attention on the need to ask these questions and to have them answered by a supervisor or by the Office of Compliance and Risk Management (OCRM).

Indeed, one area in which OCRM is most often consulted for guidance is this interface between administrators job responsibilities and their outside professional or business interests. To provide further guidance, a University Policy – The *Employee Policy on Conflicts of Interest and Outside Consulting, Employment and Other Activities* – was adopted on May 11, 2017. The purpose of this policy is to provide additional guidance to administrative employees with respect to principles embodied in the NYU *Code of Ethical Conduct* and the *Employee Policy on Conflicts of Interest.* To be noted, other conflict of interest policies apply to faculty and to trustees and designated senior administrators.

As the *Employee Policy on Conflicts of Interest and Outside Consulting, Employment and Other Activities* recognizes, administrators have expertise that may be valued by outside organizations, and association with outside organizations may benefit NYU. The policy also notes that such outside professional associations may give rise to actual, potential or perceived conflicts of interest and provides guidance on identifying, disclosing and managing such conflicts of interest.

At the outset of any discussion of conflicts of interest, it must be noted that every situation is fundamentally fact-specific and a determination as to whether it gives rise to a conflict of interest depends on the particular facts. OCRM is a resource to seek individual guidance and recommendations. Broad parameters and the kinds of facts that are relevant are contained in the policy and

Compliance Matters provides updates about important compliance issues covering new regulations, new and updated University policies, and risk management.

We welcome feedback and suggestions from the NYU Community for articles in future issues. Please send your ideas or submissions to Jessica Wasserman, Assistant Compliance Officer, at jessica.wasserman@nyu.edu.

Clearing Conflicts of Interest on the Path to Professional Enhancement (*continued from page 1)*

summarized below:

Outside Activities that do not generally give rise to conflicts of interest

Participation in work-related conferences, professional associations, advisory panels, non-profit board memberships with NYU permission, are all activities that, as the policy notes, "increase job-related skills and expertise and/or provide direct benefit to the University…." Administrators may engage in such activities with or without remuneration and/or reimbursement for related travel or other expenses after disclosing the relationship to their supervisors and obtaining prior approval, including approval to carry out such activities during work hours and using University resources.

Outside Activities that generally give rise to conflicts of interest

Outside consulting, employment or other activities may give rise to conflicts of interest if such activities involve any one of the following factual circumstances:

- The administrator is providing services outside NYU, either individually or through an entity with which the administrator is affiliated, that are similar to the administrator's job responsibilities at NYU
- The administrator, either individually or through an entity with which the administrator or a family member is affiliated, is providing, or seeking to provide goods or services to NYU
- The administrator is conducting any part of these outside activities during the administrator's normal NYU working hours, or on NYU premises, or using any NYU resources, including computers, printers, telephones, staff, and the like
- The administrator uses NYU or the administrator's employment with NYU for promotional purposes related to the outside activities
- The administrator uses or distributes NYU's confidential information and/or information that is not publically available and acquired through NYU employment
- The outside activities interfere with the administrator's NYU job performance

The Need to Disclose Potential Conflicts of Interest

As discussed in prior Newsletter articles, and stated in both the *Employee Policy on Conflicts of Interest* and the *Employee Policy on Conflicts of Interest and Outside Consulting, Employment and Other Activities*, administrators have an ongoing obligation to disclose potential or actual conflicts of interest to their supervisors. While certain designated administrators receive an annual conflict of interest disclosure questionnaire, all administrators have an obligation to disclose, and administrators who have completed the annual disclosure questionnaire have a continuing obligation to disclose any new conflicts of interest on an *ad hoc* basis when they arise. As noted, one of OCRM's primary roles is to serve as a resource for guidance on matters of conflicts of interest.

This year's annual conflict of interest disclosure will be going out to designated administrators in the beginning of 2018 through a new software platform from a third party vendor, Convercent. Any questions related to the annual disclosure may also be directed to OCRM.

Managing Conflicts of Interest

As noted in the conflict of interest policies and in prior articles, the goal of disclosure is to manage conflicts of interest. Most conflicts of interest can be managed with a conflict management plan that addresses the potential conflict of interest and develops controls to eliminate or reduce the likelihood of an actual conflict of interest. Self-fulfillment and professional fulfillment may not only coexist with our loyalties to NYU they enhance our value to NYU.

Questions or Concerns?
Call the NYU Compliance and Risk Reporting Line

NYU promotes and encourages a culture of ethical conduct consistent with laws, regulations and NYU's policies and procedures. If you have questions regarding policy violations, compliance and risk concerns, or best business practices, or if you observe conduct at NYU that is inconsistent with these expectations, we encourage you to contact the Office of Compliance and Risk Management (OCRM) directly or through the NYU Compliance and Risk Reporting Line ("Reporting Line") and website.

The Reporting Line accepts reports of conflicts of interest, financial and business integrity issues, misuse of University property or assets, wage claims, research related issues, and other compliance concerns. The Reporting Line supplements and complements, rather than replaces, other existing mechanisms and avenues for reporting employee concerns.

OCRM first launched the Reporting Line in November 2006. We are excited to announce the launch of a new anonymous reporting solution under our new vendor, Convercent. The Reporting Line still offers two easy options for you to anonymously report issues. The anonymous reporting services are available 24-hours a day, seven days a week. You may reach the Reporting Line by calling 877-360-7626 or visiting nyu.edu/reportingline to file a question or inquiry online.

Once your report has been submitted, it will be immediately forwarded to the Office of Compliance and Risk Management for review. You will also be provided a confidential issue access number and asked to provide a personal password and security question. The access number and password allow you to check the status of the report on the Convercent website as well as send and receive anonymous messages pertaining to your report at any time. If you provided an email address you will also receive email notifications from Convercent as the report status is updated.

We encourage you to use Convercent and always welcome your feedback. Please contact the Office of Compliance and Risk Management at NYUCompliance@nyu.edu or call us at 212-992-8283 directly with any comments, questions or need for support.

As a reminder, retaliatory action of any kind taken by an employee of NYU against any other employee or student of the institution as a result of that person's use of the Reporting Line is prohibited by the *Compliance Complaint Policy*, and, in certain instances, by law.

Data Privacy Laws Impacting Higher Education

Over the past few years, American organizations and individuals fell victim to a number of data breaches. Last summer, we heard about the Equifax data breach that compromised the personal data of 44% of the US population. We also learned about the WannaCry ransomware virus that infected over 200,000 computers forcing owners to pay up or lose their data. And during the last presidential election campaign hackers with ties to the Russian government hacked the Democratic National Committee. While the data breach events reported in the news tend to be larger with a broader reach, around half of security breaches are the result of human error.

There are actually two different terms that are thrown around when addressing data and information: data privacy and data security. According to technopedia.com, data privacy or protection refers to all information (e.g., electronic and paper or other mediums) and typically addresses a human element. The site defines data security as those controls or privacy measures that prevent unauthorized access to computers, databases, and websites.

NYU administrators are working hard to protect NYU data, systems, and information. It is a team effort that requires participation among all members of the NYU community. Specifically, there are a number of data privacy laws and regulations that higher education institutions, including NYU, must comply with. Below are some of the laws and regulations:

Family Educational Rights and Privacy Act (FERPA) – FERPA's purpose is to protect the privacy of students' educa-

Data Privacy Laws Impacting Higher Education

(continued from page 3)

tion records, to establish the rights of students to inspect and review their education records, and to provide students with an opportunity to have inaccurate or misleading information in their education records corrected.

Health Insurance Portability and Accountability Act (HIPAA) – HIPAA is law that addresses the privacy and security of protected health information. NYU has three covered components: School of Medicine, College of Dentistry, and the Student Health Center. HIPAA also applies to other functions. NYU developed 19 different policies, which address various areas of compliance under HIPAA.

NYS Data Breach Law – This law applies to all organizations or individuals who conduct business in the state of New York. Those conducting business in New York must report data breaches that involve a combination of personally identifiable information. Those individuals or businesses must also notify, without unreasonable delay, individuals whose information was compromised.

NYS SSN Protection Law – Prohibits certain uses and disclosures of an individual's social security number. The law also requires controls or safeguards to be implemented to protect social security numbers.

EU Data Protection Regulation (GDPR) – GDPR is a fairly new regulation. NYU is in the process of determining how to comply with these regulations. If you handle information for citizens of the European Union and would like additional information, please contact the Office of Compliance and Risk Management.

U.S. Policy for Human Subjects Research – Also referred to as the "Common Rule," this law applies to human subjects research. It requires members of the University community who engage in human subjects research not subject to exemption to: obtain prior approval from NYU's Institutional Review Board (IRB); take and pass an educational tutorial prior to commencing research; and fully inform potential subjects of the purpose and nature of the research work in which they are being asked to participate (what will be involved in participation, that under all circumstances participation is fully voluntary, and that participants are entitled to protection of their privacy) and ensure appropriate consent.

Employment Laws: Anti-Discrimination and Related Laws – There are a number of both federal and state laws that protect employees' personal information. Laws like the Americans' with Disabilities Act, Title VII of the Civil Rights Act, the Genetic Information Non-Discrimination Act, the NYS/NYC/DC Human Rights Act, and the NYC Fair Chance Act require confidential treatment and/or segregation of records.

Employment Laws: Family and Medical Leave Laws - There are a number of both federal and state laws that protect employees' personal information regarding family and medical leave. The Family Medical Leave Act (FMLA), DC Family Medical Leave Act, NYC Earned Sick Time Act, the DC Accrued Sick and Safe Leave Act of 2008, and the NYS Workers Compensation Law all require restriction of disclosure of information and/or confidential and segregated treatment of records.

This summary contains an overview of the most common data privacy laws and regulations that impact NYU operations. Please note that it is not a full list. If you would like more information, please contact the Office of Compliance and Risk Management.

Interview with Norma Kenigsberg, HIPAA Professional

Role: Program Director, IT Policy Development and Compliance (NYU IT)

Tell us a little bit more about your role in the University setting:

My title is actually quite descriptive of my broad responsibilities. Although there is overlap, I'm responsible for IT policy development and for IT compliance and act as a resource for both. I work for Kitty Bridges, Associate Vice President, Digital Accessibility/IT Policy and Compliance and also directly support Vice President and CIO Len Peters in his role as NYU's Health Insurance Portability and Accountability Act (HIPAA) University Security Officer. Throughout my 16 years at NYU, I have developed my office into a place where anyone can come to ask policy-related questions and get information regarding various regulations with which we must comply. However, my role is not legal – it's advisory and informational – and I work closely with the Office of General Counsel.

Policy development integrates with compliance in that certain policies, such as NYU's HIPAA policies, must be included in mandated training. I must keep abreast of changes in the law and how those changes affect NYU generally and NYU IT specifically. I also watch the horizon to learn what is surfacing in the regulatory world. I track changes in privacy laws for purposes of policy development, regulatory compliance, vendor relationships, employee and student training, and territorial comparison. Keeping current takes considerable time and is necessary for both my general knowledge and because I am responsible for making certain the NYU IT policies and their associated webpages are updated at least annually.

The commonality in all the regulatory requirements is the notion of privacy. Data privacy is fundamental to everything that we do. Increasingly, privacy by design – the embedding of privacy within systems and software – is taking root. Privacy and data safeguards are key considerations in all stages of any project and throughout the data lifecycle.

The *NYU IT Code of Conduct*, which was initiated in 2002 and is signed by all new NYU IT hires and annually thereafter, emphasizes the twin aspects of privacy and trust. The Code reminds us that "The principle of privacy is addressed extensively in United States federal, state, and local laws, and in various laws in the foreign countries in which NYU has global locations." And the Code states in its first paragraph that "Individuals working in NYU information technology and related areas … at New York University, at its portal campuses and global academic centers, hold positions of trust. We operate and safeguard NYU's central information technology assets, including networks, computers, telephones, access controls, information, and databases. We provide technology-related services that are vital to the smooth functioning of the University and to the members of the University community. In these roles, every one of us must adhere to the highest professional and ethical standards."

Another example of the regulatory emphasis on privacy is HIPAA in which the "minimum necessary" concept is critical. The minimum necessary standard requires HIPAA covered entities, such as NYU, to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the data use, disclosure, or request. Although adherence to the standard is sometimes easier said than done, we always must be conscious of the mandate and secure the data to maintain its privacy.

What are some key takeaways or best practices that you would like to share?

It's important to remember that the centrality of privacy will increase. The European Union's General Data Protection Regulation (GDPR) is only one example of the overarching role that data privacy will continue to play internationally for all organizations, including academic institutions. It is important to keep abreast of regulations, standards, and best practices. When it comes to privacy, the saying to "ask for forgiveness rather than permission" is unacceptable. Once

Interview with Norma Kenigsberg, HIPAA Professional

(continued from page 5)

there is a breach, there is no going back. Maintenance of good records and documentation is essential, especially when requesting or requiring information. Privacy and its necessary security safeguards should be kept in the forefront of your mind.

Are there any additional NYU resources for more information?

NYU provides quite a few resources that address data privacy and security. For example, NYU IT includes insightful articles and instructions in NYU's ServiceLink database. In addition, videos and training sessions are available through iLearn and Lynda.com. NYU iLearn also hosts a Tech Savvy suite of training sessions that cover a wide variety of topics, including an individual information security course and various applications and tools. Anyone interested in NYU IT HIPAA training is encouraged to contact Norma Kenigsberg (norma.kenigsberg@nyu.edu).

Especially important, the *Responsible Use* policy to which we all agree at login explains basic data privacy and security at NYU.

https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/responsible-use-of-nyu-computers-and-data-policy-on.html

University Policies: New and Revised

A goal of the Office of Compliance and Risk Management is to bring awareness to the NYU community about new and updated university-wide policies and guidelines. These policies are located at the University Policy Database at nyu.edu/policies.

In this issue, we highlight two new and revised policies that apply to all employees at NYU:

Anti-Bribery and Corruption Policy: The purpose of this new Policy is to ensure that members of the University community conduct University business in an ethical manner and understand and adhere to the requirements of all applicable anti-bribery laws and best practices. It is the policy of NYU to prohibit the direct or indirect giving or receiving of improper payments or other benefits for purposes of obtaining any advantage.

Global Payment Card Policy: This purpose of this revised Policy is to ensure Payment Card transactions are incurred and approved in accordance with approved University standards. Changes to the Policy include new restrictions for gift card purchases.

Global Payment Card Policy mandatory refresher training: All cardholders receiving a renewal card must complete a refresher training. The refresher training, FIN 210R, can be accessed via NYUiLearn. The FIN210R certificate is required per the *Global Payment Card Policy*. For more information about changes to the *Global Payment Card Policy*, visit the NYU FinanceLink New and Resources webpage, found here.

You can always find the most recent University policies and procedures at the University Policies and Guidelines database website.

Have Policy questions? OCRM can assist you with policy development, and add your policy to the University Policy database. Email us at NYUCompliance@nyu.edu.