HIPAA COMPLIANCE: ARE WE COVERED YET?

Gené Stephens, J.D., LL.M.
Assistant Vice-President
Compliance and Enterprise Risk Management
Office of Business and Finance
March, 2017

MIDDLE TENNESSEE STATE UNIVERSITY.

HIPAA COMPLIANCE: ARE WE COVERED YET?

Overview of Training Presentation:

I. HIPAA Privacy and Security – The Basics
   - Important Definitions
   - More on Covered Entities
   - Business Associate Contracts and Permitted Disclosures
   - Privacy and Security Rules: The Breakdown

II. FERPA, HIPAA, and the Student Health Record

III. HITECH – What is it?

IV. HIPAA and Collegiate Sports

V. Third-Party Billing Services

VI. HIPAA Penalties and Sanctions

VII. Tips & Best Practices

Let's Review! True or False?

MIDDLE TENNESSEE STATE UNIVERSITY.

I. HIPAA PRIVACY AND SECURITY – THE BASICS

The Health Insurance Portability and Accountability Act of 1996 (HIPAA or Act), Public Law No. 104-191, was enacted to improve the efficiency, portability, and continuity of health insurance coverage, as well as to provide greater security of patient health care information. The Act is divided into two main Rules: Privacy and Security.

The major elements of the Act requires the safeguarding of health information maintained and transmitted by health care providers, health plans, health care clearing houses, and other business associates involved in the continuum of patient care and in health care operations. The Act additionally provides rights and protections for patients regarding the disclosure, review, and correction of their health care records.

While detailed and extensive in scope, HIPAA is primarily designed to be both a comprehensive and flexible law that forces certain entities, known as "covered entities," to take heightened, electronic security precautions in the disclosure, transmission, and maintenance of protected health information (PHI). The Act's intersection with higher education, however, and in particular with Collegiate Sports, University Medical Centers, and business associates who perform health care administrative services for Universities, continues to be one that requires a balancing of students' educational and medical records privacy.

MIDDLE TENNESSEE STATE UNIVERSITY.

IMPORTANT DEFINITIONS

Protected Health Information (PHI). Information that is individually identifiable and that is maintained by a covered health care provider, health plan, or health care clearing house. Protected Health Information also includes genetic information under the HIPAA Privacy Rule. Covered entities are required to maintain the privacy and security of PHI except under certain, permissible circumstances. Protected health information may be disclosed for certain permissible uses, including:

1. the protection of the public health or to effectively handle a bioterrorist threat or public health emergency;
2. the administration of health care claims processing, billing, payments, and health care operations;
3. by a health care provider for continuum of care associated with a patient's treatment; and
4. for the safety, quality, and effectiveness of a Food and Drug Administration product over which a provider or medical device company has responsibility.

(45 CFR § 164.502, 506, and 512)

Covered Entity. Under the Privacy Rule, health plans, health care clearing houses, and certain health care providers are considered "covered entities" (45 CFR § 160.103). If an entity does not meet the definition of a covered entity, it does not have to comply with HIPAA.

MIDDLE TENNESSEE STATE UNIVERSITY.

IMPORTANT DEFINITIONS CONTINUED

Business Associates. Most covered entities do not perform all of their own health care functions. Instead, they contract with a variety of businesses who perform activities involving the disclosure of protected health information. Functions performed by Business Associates include: billing; payment processing; claims processing; utilization review; quality assurance; benefits management; practice management; legal; actuarial; accounting; accreditation; health care administration; and repricing (45 CFR § 160.103).

Examples of Business Associates include any of the following entities:

1. third party administrations that assist with health care or health plan claims processing, billing, and payment collections;
2. an accounting firm whose services require access to PHI;
3. an attorney whose services involve access to PHI;
4. pharmacy benefit managers who manage a health plan's pharmacy network;
5. a medical transcriptionist who provides transcription services to physicians; and
6. health care clearinghouses that translates health care claims from a non-standard format to a standard format (or vice-versa) on behalf of a health care provider (the claims are usually forwarded to a payer).

Payer (also known as a Payor). An entity that finances or reimburses the cost of health care services (other than the patient). Payers are usually employer (or union) health plan sponsors; and third-party entities who pay or reimburse the cost of health care on behalf of a plan, employer, or provider; or health insurance carriers.

MIDDLE TENNESSEE STATE UNIVERSITY.

MORE ON COVERED ENTITIES

The following are examples of Covered Entities by type. Most four-year Colleges and Universities provide at least one of the following services:

Health Care Providers
Doctor
Clinic
Psychologist
Dentists
Chiropractors
Nursing Homes
*Pharmacies *The MTSU Pharmacy is a Covered Entity under HIPAA.

Health Plans
Health Insurance Companies
Health Maintenance Organizations (HMOs)
Company Health Plans
Government health care programs, such as Medicaid, Medicare, and military or veterans health care programs.

Health Care Clearinghouses
Entities that process health information received from another entity that is typically transferred into a standard, electronic format.

MIDDLE TENNESSEE STATE UNIVERSITY.

BUSINESS ASSOCIATE CONTRACTS AND PERMITTED DISCLOSURES

Business Associate Contracts

For a covered entity who decides to utilize the services of a business associate, the HIPAA Privacy Rules require the business associate to provide assurances that it will safeguard the PHI it receives on behalf of the covered entity. The assurance must be provided in writing in the form of a "Business Associate Contract." The Act also requires the inclusion of certain Contract elements and provisions. Specifically, Business Associate Contracts must include some of the following elements (*see* 45 CFR § 164.504(e) for a full description of the requirements):

- A description of the required and permitted uses of PHI by the Business Associate.
- An assurance that the Business Associate will not use or disclose PHI other than for the uses permitted under HIPAA.
- An assurance that the Business Associate will safeguard and prevent the disclosure of PHI other than for the permitted uses by law and by Contract.
- Agreement that the Business Associate will report (to the covered entity) any use or disclosure breaches of unsecured or unprotected PHI.
- An assurance that any subcontractors used by the Business Associate agree to the same restrictions and conditions that apply to the Business Associate by law and by Contract.
- The destruction or return of all PHI received from, or created by the business associate on behalf of a covered entity at the termination of the Contract, if feasible.

MIDDLE TENNESSEE STATE UNIVERSITY.

BUSINESS ASSOCIATE CONTRACTS AND PERMITTED DISCLOSURES

Business Associate Permitted Disclosures

Among the obligations of business associates, is the disclosure of protected health information to other agencies, persons, and entities, on behalf of a covered entity in the course of health care operations. Health care operations are administrative, financial, legal, and quality improvement activities that support health care treatment and payment functions. The following are instances for which Business Associates are permitted to disclose PHI *(see* 45 CFR § 501 and 506*)*:

- Treatment
- Risk adjustments
- Payment to health care providers, health care plans, or to obtain reimbursement for provisions of care
- Determining eligibility for coverage
- Utilization review activities
- Underwriting relating to the creation, renewal, or replacement of a health insurance contract or health benefits
- Cost-management and planning
- Reviewing medical necessity
- Conducting quality assessments
- Reviewing qualification of health care professionals
- Conducting medical, legal, or auditing reviews for health care fraud and abuse detection
- Business management and general administrative activities involving compliance with and implantation of the HIPAA Privacy Rule.

MIDDLE TENNESSEE STATE UNIVERSITY.

PRIVACY AND SECURITY RULES: THE BREAKDOWN

HIPAA Privacy

The Act 's Privacy Rule established national standards to protect the use and disclosure of PHI. The Privacy Rule also permits the disclosure and transmission of PHI for covered entities.

PHI also can be disclosed by an individual who, as the subject of the health information, provides written authorization to allow the disclosure.

PHI includes:

1. An individual's demographic data;
2. An individual's past, present, or future physical or mental health condition;
3. The health care provided to an individual;
4. The past, present, or future payments provided for health care received by an individual.

There are two instances in which a covered entity must disclose PHI: (a) when the disclosure is requested by a government agency as part of a compliance investigation, review, or enforcement action, and (b) when the disclosure is specifically requested by the individual (or their representative) who is the subject of the PHI.

HIPAA Security

The Act's Security Rule establishes national requirements for covered entities (i.e. health plans, health care providers, and health care clearinghouses) when transmitting PHI electronically (called e-PHI).

Under the Security Rule, covered entities must:

1. Ensure the confidentiality and integrity of e-PHI that they create, receive, maintain, or transmit;
2. Ensure the availability of e-PHI that they create, receive, maintain or transmit;
3. Identify and protect e-PHI against reasonable, anticipated, impermissible uses and disclosures of e-PHI; and
4. Ensure their workforce complies with the Security Rule.

The Security Rule also requires covered entities to maintain certain administrative and physical safeguards to secure, identify, and analyze vulnerabilities to e-PHI including: facility access and control; workstation and device security; audit and integrity controls related to technical safeguards of e-PHI; workforce training and management regarding e-PHI security; assessment practices to evaluate the effectiveness of security policies and procedures; and security management processes.

MIDDLE TENNESSEE STATE UNIVERSITY.

II. FERPA, HIPAA, AND THE STUDENT HEALTH RECORD

The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR § 99, governs the access to, and disclosure of, students' educational records and provides students with certain rights. Eligible students (students who reach the age of 18 or who attend a postsecondary institution) are allowed to inspect, review, obtain copies of, or request that corrects be made to their educational records.

Because "educational records" are broadly defined under FERPA, student health records often are thought to be subject to HIPAA Privacy rules. For FERPA purposes, "educational records" are directly related to the student, and are maintained by an educational agency or institution or by a party acting for the agency or institution (34 CFR § 99.3).

Although excluded from the definition of educational records, students' treatment records (which include health or medical records) are also governed under FERPA if:

1. The records were made or maintained by a university physician, psychiatrist, psychologist, or other recognized professional; or
2. The records were made, maintained, or used in connection with the provision of treatment to a student and the records are not available to anyone other than the persons providing treatment, except for the student's physician or other appropriate professional of the student's choice.

In addition, in order for a university or institution to disclose students' treatment records for other purposes, the institution may do so with prior, written consent from the student. If students' treatment information is disclosed to a third-party, health care provider, or other HIPAA covered entity (such as a health plan, health care billing service, or a health care clearing house), the students' records, and the disclosure of those records to the covered entity, would be governed by, HIPAA Privacy rules.

MIDDLE TENNESSEE STATE UNIVERSITY.

II. FERPA, HIPAA, AND THE STUDENT HEALTH RECORD CONTINUED

A key question to consider and ask when determining whether a student's record is covered under FERPA or HIPAA is:

- ***Was the record made, maintained or used only in connection with the treatment of a student?***

  If the answer is 'Yes,' and the record was made or maintained by a college or university-run clinic or medical center, FERPA governs the record.

To determine if HIPAA applies to a record made or maintained by a university or college clinic, medical center, or hospital, ask:

- **Is the medical center or health care service open and available to non-student patients?**

  If the answer is 'Yes,' than the record is subject to both FERPA *and* HIPAA rules because the medical center is open to non-students (i.e. faculty, staff, and others). In this case, the student records would be governed under FERPA (this is particularly true where the medical center is run on behalf of the University), and the non-student records would be covered under HIPAA. An example, is a pharmacy that is run by a university or college, but whose pharmacy services includes services to university faculty, staff, and non-university related community members (all of whom are non-students).

- **Is the record being disclosed or transmitted to a HIPAA covered entity?**

  If the answer is 'Yes,' then HIPAA is triggered.

MIDDLE TENNESSEE STATE UNIVERSITY.

III. HITECH – WHAT IS IT?

In 2009, the HIPAA Privacy and Security Rules were expanded with the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH's regulations placed additional requirements on business associates and covered entities for the enhanced protection of PHI and electronic PHI (e-PHI) (42 CFR § 164.308-312, and 164.316).

Specifically, HITECH expanded HIPAA Privacy and Security Rules by:

1. Requiring Business Associates to directly comply with HIPAA Privacy and Security rules related to the implementation of administrative, physical, and technical safeguards of e-PHI (just like the covered entities with whom they contract).

2. Requiring Business Associates to comply with HIPAA's business associate safeguards, which includes limiting the use and disclosure of PHI; making books and records available to the federal Department of Health and Human Services (DHHS;, and returning or destroying PHI at contract termination, if feasible.

3. Requiring Business Associates to provide access to, and an accounting of, HIPAA disclosures.

4. Expanding the accounting requirements related to health records.

5. Restricting the disclosure of health information to health plans.

6. Revising the prohibition on the sale of PHI.

7. Limiting marketing and fundraising communications by covered entities and business associates that encourages individuals to purchase a product or service were updated.

8. Enhancing civil and criminal penalties for non-compliance with HIPAA/HITECH.

MIDDLE TENNESSEE STATE UNIVERSITY.

III. HITECH – WHAT IS IT? CONTINUED

HITECH additionally requires business associates to report instances of non-compliance to United Department of Health and Human Services (DHHS) whenever the business associate knows of a pattern of activity or practice by a covered entity that breaches a business associate agreement, fails to cure the breach of a business associate agreement, or fails to terminate the agreement (42 CFR § 164.504(e)(1)(u). Lastly, and it relates to HIPAA Security, HITECH provides tougher data security requirements for both covered entities and business associates.

The expanded regulations under HITECH became effective in 2010 (42 U.S.C. § 17931, et seq.).

For universities and colleges that provide health care services to non-students, or where the university or college contracts with a covered entity to provide, or manage, health care administrative services as defined under HIPAA, careful attention must also be given to HITECH's requirements. Thus, failing to comply with HITECH may also mean a compliance violation of HIPAA.

IV. HIPAA AND COLLEGIATE SPORTS

"Depending upon the status of a team physician for college teams, there are different stipulations about what information can be shared. Some team physicians conduct part of their practice through the student health center. In this case, the physician falls under the guidelines of FERPA and should be allowed to share information with coaches and athletic trainers. A physician not employed by a university-run health center will be subject to the HIPAA guidelines. In this case, it is possible that…[for] any information to be released to athletic trainers, an authorization form would need to be signed. An exception to HIPAA exists that specifically states that information can be released to another provider for treatment purposes. What is unclear, however, is whether or not a trainer is considered a provider under HIPAA guidelines."

D. Hill, *A matter of privacy*, Athletic Management, 15(2), 37-42 (2003); and *The Impact of the HIPAA Privacy rule on Collegiate Sport Professionals*, The Sports Journal, United States Sports Academy, ISSN: 1543-9518 (April 2, 2008).

The excerpt from the above quote speaks to the ongoing tension between HIPAA Privacy and Security rules and the needs of Collegiate Sports departments to update its fans and constituents on the health status of student-athletes while ensuring athletes receive quality, medical treatment for the student's safety and well-being.

Athletics departments were never meant to be medical clinics or covered entities. However, most university athletics departments have athletics trainers, physicians (whether employed by the university or as independent contractors), and other medical personnel who regularly treat student athletes. The treatment of collegiate athletes also means medical billing, collections, payment processing, and health care accounting – all of which fall under the health care operations definition of HIPAA. In most cases, universities also contract with third parties to perform health care administrative duties.

Whenever a university's athletic departments submits a bill, charges for health services, or electronically transmits PHI to a HIPAA covered entity (such as a health plan or state health program), HIPAA is triggered (*see also,* Walker, Travis. *The Price of Health Privacy in Sports*, The University of Utah S.J. Quinney College of Law, *BiolawToday.org* (Nov. 12, 2015)).

HIPAA also can be triggered whenever a university or college athletics department elects to contract with a third-party to perform health care administrative services. While treatment records in collegiate sports fall under FERPA because they are records made, maintained, and used for the treatment of student athletes, universities and colleges walk a fine line regarding the HIPAA trigger whenever, (1) their athletics department contracts with a covered entity under HIPAA, or (2) there is disclosure of a student athlete's health information to the public or media without the student's written release or consent for such disclosure. Therefore, careful attention must be given to agreements between collegiate sports departments and covered entities who would do business with those departments. Such attention also helps ensure that certain compliance elements are in place for the university if HIPAA becomes triggered as part of any agreement.

MIDDLE TENNESSEE STATE UNIVERSITY.

V. THIRD PARTY BILLING SERVICES

Third Party Billing Services

Combatting fraud, abuse, and waste in health care continues to be one of the major efforts and goals of the federal Office of the Inspector General (OIG). Since third-party medical billing companies provide a host of health care administrative services on which other covered entities, business associates, providers, and others rely, a review of the safeguards established by such companies is as important as a covered entity's own internal controls.

The OIG provided guidance to third party medical billing companies in December 1998 when it recommended that such companies should follow the seven (7) fundamental elements of a compliance program. The OIG also outlined the benefits of having a compliance program (see 63 FR 70138 - 70145 (Dec. 18, 1998)). Additionally, the OIG identified key areas of third party medical billing that tend to be vulnerable to health care fraud and abuse. Some vulnerable areas and practices of third party billing services include the following:

- billing for items or services that are not actually documented;
- unbundling (i.e. fragmenting or submitting medical bills piecemeal to maximize health care reimbursement);
- upcoding (i.e. billing or medical coding a bill for a more expensive service than the medical service performed);
- inadequate resolution of overpayment;
- inappropriate balance billing;
- knowing misuse of provider identification numbers, which results in improper billing;
- duplicate billing in an attempt to obtain duplicate payment;
- routine waiver of copayments, and billing third-party insurers only;
- discounts and professional courtesy;
- failure to maintain the confidentiality of information and records;
- computer software programs and systems that encourage billing personnel to enter data in fields indicating services were rendered that were not actually performed or documented;
- billing for discharge in lieu of transfer; and
- joint ventures (i.e. business arrangements that may violate the Anti-Kickback statute in which one company is in a position to refer business to another, such as to a provider physician.

MIDDLE TENNESSEE STATE UNIVERSITY.

VI. HIPAA PENALTIES AND SANCTIONS

The enforcement penalties and sanctions under the HIPAA Privacy and Security Rules are steep. There are both civil and criminal penalties for violations of HIPAA. The DHHS and Office for Civil Rights (OCR) is responsible for enforcing HIPAA Privacy and Security rules, and the OIG investigates HIPAA violations, as well as investigates cases involving health care fraud and abuse and violations of other health care compliance laws.

Civil Penalties: The Costs of Non-Compliance

Civil monetary penalties (CMPs) for HIPAA violations are assessed on a tiered structure based on an individual's or entity's knowledge of HIPAA or willful neglect of compliance with the Act. If an individual or entity corrects a HIPAA violation within 30 days of the violation or within the required time period set by the government, and except in cases of willful neglect of the Act, the DHHS Secretary is prohibited from imposing a civil penalty.

The information below illustrates the costs of non-compliance with HIPAA Privacy and Security *(ref.* American Medical Association, *HIPAA Violations & Enforcement*, available at www.ama-assn.org/practive-management/hipaa-violations-enforcement.

Violation Type	Minimum Penalty	Maximum Penalty
Unknowing	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Reasonable cause (to know)	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Willful neglect, but the violation is corrected within the required time period (usually 30 days or more at DHHS's discretion)	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Willful neglect and is not corrected within required time period	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

MIDDLE TENNESSEE STATE UNIVERSITY.

VI. HIPAA PENALTIES AND SANCTIONS CONTINUED

HIPAA Complaint Resolution

In the case of Civil Penalties, covered entities can resolve and mitigate penalties through voluntary compliance, corrective action plans, and/or a resolution or integrity agreement with OCR.

Criminal Violations

In addition to civil penalties, violations of HIPAA carry criminal penalties, which are handled by the Department of Justice (DOJ). Similar to the tiered structure of the civil penalties, criminal violations also have levels based on severity of the criminal activity.

Individuals and entities who knowingly obtain or disclose individually identifiable health information can be fined up to $50,000, as well as face up to one (1) year of imprisonment. Additional criminal offenses are assessed for individuals or entities who conduct business under false pretenses involving HIPAA Privacy and Security. In such cases, the criminal fine increases to $100,000 with up to five (5) years imprisonment. In addition, individuals or entities who attempt or intend to sell or transfer PHI for personal gain, malicious harm, or commercial advantage can be fined $250,000 and imprisoned up to ten (10) years.

Covered entities also can be excluded from participation in federal health care programs (Medicare and Medicaid) for HIPAA violations.

The Lesson

Establishing controls, policies, and procedures for protecting individually identifiable health information can save an organization or individual from unnecessary expense, as well as potential imprisonment. Therefore, It is important to review agreements and other arrangements, including business associate agreements, in which HIPAA is, or may be, triggered. Taking reasonable and appropriate measures to institute administrative, technical, and physical safeguards of PHI and the transmission of PHI or other health care operational information can reduce an organization's or covered entity's risk and liability.

MIDDLE TENNESSEE STATE UNIVERSITY.

VII. TIPS & BEST PRACTICES

There are ways individuals and businesses can prevent violations of HIPAA compliance in every day practice. While the government provides a definition for covered entities, compliance with HIPAA Privacy and Security extends well beyond health care providers, health plans, and health care clearing houses. Even universities and colleges can be subject to HIPAA rules and other health care regulations and statutes based on their business interactions with HIPAA covered entities.

The following is a list of best practices to ensure compliance with HIPAA Privacy and Security rules and to minimize risk and liability (*see also* Zabel, Laurie. *10 Common HIPAA Violations and Preventative Measures to Keep Your Practice in Compliance*, Becker's Health IT & CIO Review (June 22, 2016), *also available at* www.beckershospitalreview.com).

1. **Be Mindful.** Ensure employees are mindful of their environment when discussing patient information, including treatment, testing, or medical records information.
2. **Minimum Use and "Need to Know."** Only employees and/or other health care providers or administrators who need to know a patient's information for the provision of care or for health care operational purposes should have access to patient health records.
3. **Handle with Care.** Avoid mishandling patient records, which can include leaving a patient record or chart in an exam room for another patient to see; leaving a medical record in a common area that is used by others or in high traffic; or leaving a portable device containing protected health information unlocked and in an open space that can expose the device to theft.
4. **Social Media.** Ensure employees understand that posting patient information or patient photos on social media is a HIPAA violation.
5. **Home Access.** Avoid accessing patient information on home computers, as this could potentially result in HIPAA Privacy and Security violations if: (a) the screen can be viewed by other family members; (b) the security settings on the home computer are not compliant with HIPAA Security and HITECH standards; and/or (c) the laptop lacks the government required encryption tools needed to secure patient information.
6. **Before You Sign, Understand.** Carefully review agreements with business associates, covered entities, and/or third party billing services to ensure that both the agreement complies with HIPAA Privacy and Security rules and that the organization has controls and safeguards in place within its health care operations.
7. **Training is Key.** Organizations should ensure that training is available to all employees who are not familiar with HIPAA regulations. The training should include a discussion of the risks, violations, and penalties associated with HIPAA compliance.

MIDDLE TENNESSEE STATE UNIVERSITY.

LET'S REVIEW!

MIDDLE TENNESSEE STATE UNIVERSITY.

Let's review your knowledge of HIPAA Privacy and Security compliance…

1. Knowingly misusing a provider's identification number can trigger a health care fraud and abuse violation because such action can result in improper medical billing. **True or False?**
2. Violations of HIPAA Privacy and Security only result in civil monetary penalties. **True or False?**
3. HITECH is a new social media site and is used like Snapchat. **True or False?**
4. Business associates are held to the same HIPAA Privacy and Security compliance standards as covered entities. **True or False?**
5. "HIPAA" stands for the Health Insurance Protection and Accessibility Act. **True or False?**
6. HIPAA Privacy and Security rules are the same. **True or False?**
7. Universities and Colleges also can be subject to HIPAA compliance in some situations. **True or False?**
8. A University medical center or pharmacy that provides health care services to non-students is subject to HIPAA. **True or False?**
9. A University medical center or pharmacy that provides health care services to students, and that makes and maintains health care records solely in connection with the treatment of students, is covered under HIPAA. **True or False?**
10. "E-PHI" stands for "Electronic Protected Health Information." **True or False?**
11. PHI and other medical records should be kept on portable devices, such as laptops, mobile phones, and IPads for ease of transport. **True or False?**

MIDDLE TENNESSEE STATE UNIVERSITY.

QUESTIONS?

For questions regarding this presentation, contact Gene.Stephens@mtsu.edu or mail your questions to:

Gené Stephens, J.D., LL.M.
Assistant Vice-President for Compliance and Enterprise Risk Management
Middle Tennessee State University
Cope Administration Building, 119
1301 E. Main Street
Murfreesboro, TN 37132