Northern Arizona University
Employee, Trainee, Intern, Volunteer
Security and Confidentiality Agreement

As an employee, trainee, intern, or volunteer of Northern Arizona University, and as a condition of my employment, training, or volunteer work, I agree to the following:

1. I understand that I am responsible for complying with Northern Arizona University HIPAA policies**,** which were provided to me in my training on_____.

2. University and HIPAA policies apply to protected health information. All requirements in this "Employee Security and Confidentiality Agreement" referencing "patients" apply to both "patients" and "clients".

3. I understand that I may have access to patients' protected health information in the course of my duties. I will respect the privacy of the patients and I will preserve the privacy, confidentiality and security of their protected health information. This information could be in any format, including, but not limited to: oral, written, fax, electronic or photographic information.

4. I will access patient information only to the minimum extent necessary to perform my assigned duties. I will not read or access protected health information that has not been authorized in the scope of my duties. I will not attempt to access a secure application or restricted area without proper authorization.

5. I will disclose protected health information to other persons or entities only as necessary to perform my assigned duties, and as specifically permitted under University and HIPAA policies. If I am unsure as to what information can be disclosed, or to whom it can be disclosed, I will ask my supervisor prior to disclosing the information. If I am still unsure as to what information should be disclosed, I will ask the University Privacy Officer for clarification.

6. I will be discrete when talking to or about patients. I will speak quietly, and will take a patient to a private area if necessary to maintain privacy. I will avoid using patients' names in public areas.

7. I will not alter or delete protected health information without specific written authorization from the University Privacy Officer.

8. I will not log on to any of the computer applications that currently exist, or may exist in the future, using an employee ID or password other than my own. I will safeguard my computer password(s) and will not post password(s) in a visible place, such as on the computer monitor or in a place where it will be easily lost. I will not allow anyone, including other employees, to use my password(s) to log on to computer application(s). I will not provide any unauthorized person with access codes for files, accounts or restricted areas, whether electronic or physical. I will not leave a secure application unattended. I will log off of the computer, or computer application(s), as soon as I have finished using it.

9. I will not use e-mail to transmit patient information unless I am instructed to do so by my supervisor or the University Privacy Officer, and will ensure that it is done using a secure,

encrypted transmission, such as through the secure messaging system in an electronic medical record application.

10. I will not take protected health information from the premises in paper or electronic form, without first receiving authorization from the University Privacy Officer. I will not copy protected health information onto paper or onto any removable electronic device, or onto an unsecure application, without first receiving authorization from the University Privacy Officer.

11. I will IMMEDIATELY notify my supervisor and the University Privacy Officer, of any unauthorized use or disclosure of protected health information, whether intentional or unintentional. I understand that the University may be required to report unauthorized use or disclosure of protected health information to the Department of Health and Human Services Office of Civil Rights, as required by law.

12. I will IMMEDIATELY notify my supervisor and the University Privacy Officer of any concerns or issues affecting the security of protected health information.

13. Upon cessation of my employment or training with the University, I agree to continue to maintain the confidentiality of any information I learned while an employee or trainee, and agree to turn over any keys or any other device that would provide access to information.

14. I understand that violation of HIPAA is a violation of federal and state law, and may result in civil and criminal penalties including, but not limited to, the following:

    Civil Penalties: Includes fines from $100 to $50,000 per violation per person, with a maximum total fine of $1,500,000 for all violations of the same requirement or prohibition in a calendar year.
    (Applies to the covered entity).

    Criminal Penalties: Can include fines and jail time as follows:
    (Applies to the individual and the entity).
    - Knowingly releasing PHI in violation of HIPAA can result in a fine of up to $50,000, up to a year in prison, or both;
    - Gaining access to PHI under false pretenses (for example, misrepresenting yourself as a physician so you can see a patient's medical record) can result in a fine of up to $100,000, a maximum of a 5-year prison sentence, or both; and
    - Releasing PHI with harmful intent or selling PHI (for example, selling PHI about a famous patient to the media) can result in a maximum fine of $250,000, a prison sentence of up to 10 years, or both.

I understand that violation of this agreement could result in disciplinary actions up to and including termination, personal, civil and/or criminal and legal penalties.

_____ _____

Name (signature) Date

_____ _____

Name (printed) Position