Department:_____

HIPAA Security
Competency Checklist

Employee Name:_____
Employee UID:_____

Instructions: Competency checklist to be used during annual evaluation and at time of departmental orientation.

Competency or Educational Item	Yes	No	Init
Received HIPAA Security training during general orientation or at E&C refresher in last 12 months.			
Do you know that passwords should a minimum of 7 characters and comprised of 3 of the following 4 items: lower-case alpha, upper-case alpha, numeric, and special characters?			
Do you know how to construct passwords that are not easily guessed?			
Do you know never to share your password and to never use another person's password?			
Do you know to never open an attachment in an email message that you are unsure of who the sender is, and to report any potential viruses to the help desk?			
Do you know to contact the FISO or ECO if you suspect any form of security incident? This could include viruses, password or media violations, inappropriate use of system, etc.			
Do you know to back up all your mission critical files either file servers or local media, and to store in a secure location. I am responsible for assuring my personal files are safe.			
Do you know to access information on only a need-to-know basis regardless of access rights?			
I know to label all media as confidential if I move any sensitive data to CD, USB drive, tape, etc.			
I know that all computer software must be owned and licensed by OUM and installed by the IS department, and to never download software from the Internet without permission from IS.			
Do you know to use E Mail and the Internet responsibly and productively to facilitate company business and maintain and enhance the company's image and reputation?			
Do you know to keep a copy of any official Company business records you originate in a mailbox folder or hard copy?			
I will not send ePHI or sensitive company information outside of OUM unless it is encrypted to protect it from unauthorized access. I will notify IS if I need those tools.			
I understand I am held accountable for protecting all ePHI and that violations are subject to disciplinary action up to termination.			
I will use password protected screen savers and assure my computer is physically secure.			
I know where to find OUM Security policies.			
I understand that all media, CD's, USB drives, tapes, and other removable media are not to be thrown away. I know to dispose of all removable media through the IS department.			
I know to challenge anyone accessing a computer system or entering a secure area who I suspect should not be.			
If I must leave a workstation unattended, I understand I am to log off the application and workstation or I must secure the workstation by locking it through Windows or a password-protected screen saver.			

_____ _____

Employee Signature/Date Director or Manager Signature/Date

Revised 3/5/18