HUMAN RESOURCES

UNIVERSITY PARTNER PACKET

INSTRUCTIONS: Board of Regents - University of Oklahoma Division Contact to complete page 1-4 electronically, University Partner to complete page 5-9 in legible fashion. Board of Regents - University of Oklahoma Division Contact to remit fully completed Packet to ContractWorkers@OUHealth.com with completed Compliance Roster, required Licensure and Certification, and signed Job Description.

UNIVERSITY CONTACT INFORMATION, UNIVERSITY PARTNER INFORMATION, AND ACKNOWLEDGEMENTS

UNIVERSITY CONTACT INFORMATION

University Contact Division

University Contact Full Name

University Contact Email Address

University Contact Phone Number

University Contact Position

UNIVERSITY PARTNER INFORMATION

Legal First Name

Legal Middle Name

Legal Last Name

Address

City

State

Zip Code

Email

Phone Number

Date of Birth

Emergency Contact

Emergency Contact's Phone Number

Position

UNIVERSITY CONTACT ATTESTATIONS AND ACKNOWLEDGEMENTS

Training and Competency Attestation

Initialed Acknowledgement

University Partner has reviewed training as located on the OU Health Contingent Worker Website, to track compliance and training received, the Training Version used is noted below.

Training Version:

On behalf of the University listed above, I acknowledge and attest that we own and have in our possession satisfactory training records to establish that University Partner is trained and qualified for the Position identified above. If University Partner is fulfilling a clinical position, Board of Regents - University of Oklahoma has completed initial skills check-offs to validate competency in required skills of position. If University Partner works with Board of Regents - University of Oklahoma for greater than a year, annual training to recertify competencies is required.

This attestation is provided in lieu of providing a copy of the training and competency validations.

Satisfactory Background Investigation Report Attestation

Initialed Acknowledgement

On behalf of the University listed above, I acknowledge and attest that we own and have in our possession a background investigation report on the individual identified above. Such background investigation is satisfactory in that it:

- Does not reveal any criminal conviction that has not been disclosed to OU Health;
- Confirms candidate meets the minimum education or experience qualifications, as stated on the current job description;
    - If an RN, Board of Regents - University of Oklahoma can confirm through primary source verification, that the RN has completed the following degrees:

	ADN	BSN	MSN	DNP
Year Graduated				

- Confirms the individual is not listed as a violent crime or sexual offender;
- Confirms the individual is not on the GSA or OIG exclusion lists;
- Confirms this individual is not on the U.S. Treasury Department's Office of Foreign Assets Control list of Specially Designation Nationals; and

I further attest that the background investigation report does not include any information about prior or pending investigations, reviews, sanctions or peer review proceedings; or limitations of any licensure, certification or registration.

This attestation is provided in lieu of providing a copy of the background investigation report.

Immunization and Health Attestation

Initialed Acknowledgement

On behalf of the University listed above, I acknowledge and attest that we own and have in our possession health records that substantiate the information provided below. Information provided below reflects the date the immunizations were received by University Partner, Titer results were received from lab, or date declination form is signed by University Partner.

	Immunization #1	Immunization #2	Immunization #3	Positive Immune Titer	Declination
Hepatitis B					
Measles					
Mumps					
Rubella					
Varicella					

	PPD Negative Reactive Date OR Negative Infection Blood Test Date (results must be within the last year)	If Past Positive, Negative Chest X-Ray Date (results must be within the last two years)
Tuberculosis Testing		

University Partner must have either Immunizations, Positive Immune Titer or Declination Form as options avail above. Tdap expires every 10 years and updated date on the Compliance Roster must be provided prior to expiration. Participation in COVID-19 and Influenza is required and tracked on the Compliance Roster with most recent dates, which could be through immunization or declination. Declination Forms are held on the OU Health Contingent Worker Website.

This attestation is provided in lieu of providing a copy of the immunization records upon onboarding.

Application Attestation

Initialed Acknowledgement

On behalf of the University listed above, I acknowledge and attest that we own and have in our possession an application submitted on behalf of the individual identified above, if applicable. The application in our possession must include work and education history.

If requested, the application will be provided to OU Health.

Performance Evaluation Attestation

Initialed Acknowledgement

On behalf of the University listed above, I acknowledge and attest that the individual identified above maintains and meets the annual performance requirements of the position with OU Health.

If requested, the copies of performance evaluations will be provided to OU Health.

Drug Test Acknowledgement

Initialed Acknowledgement

On behalf of the University listed above, I acknowledge that a 10 panel drug test will be administered by OU Health and to retain employment at an OU Health facility the individual identified above must be cleared satisfactorily. The drug test results includes all of the following Amphetamines, Cocaine, Marijuana, Opiates (to include Synthetic Opiates), Propoxyphene, Benzodiazepines, Methaqualone, Methadone, Phencyclidine, and Barbiturates.

Job Description Attestation

Initialed Acknowledgement

On behalf of the University listed above, I acknowledge and attest that we own and have in our possession a signed copy of a job description submitted on behalf of the individual identified above. The signed job description on file includes minimum qualifications, required competencies, and physical essential functions for the contracted position.

If the individual listed above is fulfilling a job description that is held by OU Health, the OU Health job profile must be retained by the Board of Regents - University of Oklahoma in a signed, dated, and accepted manner by the University Partner. Board of Regents - University of Oklahoma must also remit the signed, dated, and accepted Job Description to OU Health.

If requested, the signed copy of the job description will be provided to OU Health to validate retention of the Board of Regents - University of Oklahoma.

Licensure and Certification Attestation

Initialed Acknowledgement

On behalf of the University listed above, I acknowledge and attest that we own and have in our possession active Primary Source Verification of any legally-required or hospital-required licensure, registration, and/or certification submitted on behalf of the individual identified above. Verifications will be conducted initially, when the credential expires, and upon renewal. Actions are taken to ensure that no one works at OU Health without a legally-required or hospital-required credential. Expired required License or certifications may be subject to termination of University Partner contract.

Upon each Primary Source Verification, a copy will be remitted to ContractWorkers@OUHealth.com.

Company Agent Acknowledgement

I hereby attest that the individual sent to work in or on the premises of OU Health is legally permitted to work in United States. I also acknowledge and agree to an annual compliance audit by the employer of five percent (5%) or a minimum of thirty (30) such background investigation files as authorized by the subjects under the Fair Credit Reporting Act (FCRA). Actual employee files may be requested by OU Health for audit or inspection at any time.

Board of Regents - University of Oklahoma will document and verify worked hours of the above individual as OU Health may also request documentation to verify hours worked. Board of Regents - University of Oklahoma acknowledges that individuals who work over 160 hours in a calendar year are required to complete trainings per OUM Policy HR.083.

Also, Board of Regents - University of Oklahoma agrees to be responsible for employees conduct, including negligent conduct.

Signature	Date

UNIVERSITY PARTNER INFORMATION AND ACKNOWLEDGEMENTS

Legal First Name	Legal Middle Name	Legal Last Name

Prior Employment or Access

Please check one:

- ☐ I was previously employed/contracted to OU Health
- ☐ I was **NOT** previously employed/contracted to OU Health

When I was previously employed with OU Health (or related entities) or contracted to preform services through a third party at an OU Health facility, I was employed through the following employer:

Prior Employer:		Approx. Date(s):	

If previously employed or contracted, my 3/4 ID is:

3/4 ID:	

PACCT: People | Accountability | Collaboration | Compassion | Transparency

OU Health strives to live by the PACCT, which includes the following standards:

- To respect **People** we serve and serve with,
- To be **Accountable** to them, to ourselves and to our communities, to passionately deliver excellence in patient care, education, and research,
- To be **Collaborative** and **Compassionate** in all our efforts, and
- To be **Transparent** and act with integrity in all of our work as a premier academic health system.

In service to our patients and colleagues, I agree with the PACCT and agree to uphold, role model and integrate it in every aspect of my work.

Please check one:

- ☐ I agree
- ☐ I do not agree

Policy and Procedures Attestation and Agreement

I understand that I have access to OU Health Policies and Procedures via the OU Health Intranet or directly through Human Resources in the OUMC Clinics Building located at 711 Stanton L Young Blvd, Suite 103, Oklahoma City, OK 73104. I agree to abide by OU Health policies and use them to guide my actions in my role within the facility.

Please check one:

- ☐ I agree
- ☐ I do not agree

HIPAA/HITECH Privacy Training

I acknowledge that I have reviewed the HIPAA/HITECH training. I also agree that I will ensure the safety of our patient's Protected Health Information for every patient, every time.

Please check one:

- ☐ I agree
- ☐ I do not agree
- ☐ I need to discuss further with my supervisor or HR representative

Infant Security Attestation

I have read and understand the Infant Security Policy and I understand that, like all OU Health and departmental policies, I am expected to practice to that standard at all times. I understand that if I have questions or concerns about the policy or its implementation, I can consult my supervisor or other leaders for clarification and direction.

Please check one:

- ☐ I agree
- ☐ I do not agree

HIPAA Security Competency Checklist

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

- 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.

Please check one:

☐ I agree
☐ I do not agree

Confidentiality and Security Agreement

I understand that OU Health and its affiliated facilities and entities (collectively, "OUH" or the "Company") manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information.

Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, credentialing, intellectual property, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment/assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company systems.

General Rules

- I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
- I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
- I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.

Protecting Confidential Information

- I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
- I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
- I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards and Company record retention policy.
- In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to

protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.

- I will not make any unauthorized transmissions, inquiries, modifications, or purging of Confidential Information.
- I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Company using email or other electronic communication methods, I will ensure that the Information is encrypted according to Company Information Security Standards.

Following Appropriate Access

- I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
- I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

Using Mobile Devices, Portable Devices and Removable Media

- I will not copy or store Confidential Information on mobile devices, portable devices or removable media such as laptops, personal digital assistants (PDAs), cell phones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so by my job. If I do copy or store Confidential Information on removable media, I will encrypt the information while it is on the media according to Company Information Security Standards.
- I understand that any mobile device (Smart phone, PDA, etc.) that synchronizes company data (e.g., Company email) may contain Confidential Information and as a result, must be protected as required by Company Information Security Standards.

Doing My Part – Personal Security

- I understand that I will be assigned a unique identifier (e.g., 3-4 User ID) track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
- I will:
    - Use only my officially assigned User-ID and password (and/or token).
    - Use only approved licensed software.
    - Use a device with virus protection software.
- I will never:
    - Disclose passwords, PINs, or access codes.
    - Allow another individual to use my digital identity (e.g., 3-4 User ID) to access, modify, or delete data and/or use a computer system.
    - Use tools or techniques to break/exploit security measures.
    - Connect unauthorized systems or devices to the Company network.
- I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords, positioning screens away from public view.
- I will immediately notify my manager, OUM Information Security Official , OUM Director of Information Technology, or OUM help desk if:
    - my password has been seen, disclosed, or otherwise compromised;
    - media with Confidential Information stored on it has been lost or stolen;
    - I suspect a virus infection on any system;
    - I am aware of any activity that violates this agreement, privacy and security policies; or
    - I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

- I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.

- Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
- I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Please check one:

- ☐ I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.
- ☐ I do not agree
- ☐ I need to discuss further with my supervisor or HR representative

Acknowledgement

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated therein.

Printed Name

Signature

Date