EXHIBIT H

CONFIDENTIALITY AGREEMENT FOR WORKFORCE MEMBERS WHO ARE CONSULTANTS, CONTRACTORS OR VENDORS

I understand that I require information to perform my duties at the Johns Hopkins University or Johns Hopkins Health System entity by which I am engaged or for which I am performing services ("Johns Hopkins"). This information may include, but is not limited to, information on patients, employees, students, other workforce members, donors, research, and financial and business operations (collectively referred to as "Confidential Information"). Some of this information is made confidential by law (such as "protected health information" or "PHI" under the federal Health Insurance Portability and Accountability Act) or by Johns Hopkins policies. Confidential Information may be in any form, e.g., written, electronic, oral, overheard or observed. I also understand that access to all Confidential Information is granted on a need-to-know basis. A need-to- know is defined as information access that is required in order to perform my work.

By signing below, I agree to the following:

- I will not disclose Confidential Information to patients, friends, relatives, co-workers or anyone else except as permitted by Johns Hopkins policies and applicable law and as required to perform my work as a consultant, contractor or vendor for Johns Hopkins.

- I will not post or discuss Confidential Information, including pictures and/or videos on my personal social media sites (e.g. Facebook, Twitter, etc.). Likewise, I will not post or discuss Confidential Information on Johns Hopkins-sponsored social media sites without the appropriate authorization in accordance with established Johns Hopkins policies and procedures.

- I will not access, maintain or transmit Confidential Information on any unencrypted portable electronic devices (e.g. Blackberries, Androids, iPhones, iPads, etc.) and agree to use such devices in accordance with Johns Hopkins policies only.

- I will protect the confidentiality of all Confidential Information, including PHI, while at Johns Hopkins and after I leave Johns Hopkins. All Confidential Information remains the property of Johns Hopkins and may not be removed or kept by me when I leave Johns Hopkins except as permitted by Johns Hopkins policies or specific agreements or arrangements applicable to my work as a consultant, contractor or vendor for Johns Hopkins.

If I violate this agreement, I may be subject to adverse action up to and including termination of my ability to work at or on behalf of Johns Hopkins. In addition, under applicable law, I may be subject to criminal or civil penalties.

I have read and understand the above and agree to be bound by it.

Name: _____ Company: _____

Signature: _____ Date: _____

Johns Hopkins Dept/School for which providing services: _____

Privacy and Security Tips and Reminders

- Avoid disclosing unencrypted electronic PHI in e-mails and shared files over the Internet.
- Never share your log-in with another user.
- Never store electronic PHI on a handheld or portable device that is unencrypted.
- Access and use only the PHI needed to do your job.
- Log off or lock your computer when you are not using it.
- Report computer security problems quickly.
- Report lost or stolen PHI or electronic PHI as soon as possible.

A 3 3 a Effec. Date