Discussion Tool for Chairs and Directors
Annual Review of the Privacy, Confidentiality and Information Security Agreement (PCISA)

The PCISA is used to inform UW Medicine workforce members about their responsibilities for protecting confidential (regulated patient, student, financial, personal, or proprietary information) and restricted (other protected but not regulated data). The document must be signed upon hire, reviewed and signed annually thereafter or when there is a change in jobs, and retained in the workforce member's personnel file. The annual review enables individuals with management and supervisory responsibilities to understand the type of information workforce members use and reinforce role-specific expectations for how that information is handled. It also provides the workforce member and manager/supervisor with a shared understanding of the risks and the safeguards that are needed.

The following is an outline of questions and topics to cover when annually reviewing data stewardship with your faculty and staff. Retain your notes of each discussion with the signed PCISA. If, when reviewing your notes, you find common issues for which you want additional training for your employees, please contact the UW Medicine ITS Security Team at uwmed-security@uw.edu.

Discussion with: _____ Date: _____
Employee's Name

Supervisor/Manager: _____ Title: _____
Supervisor/Manager's Name

What type of information do you handle during the course of your work?

☐ Confidential Information: data that is regulated or protected by law:

- Protected Health Information (PHI) - protected by HIPAA ____ YES ____ NO
  - If so, has required training been taken? ____ YES ____ NO
  - Does this employee need refresher training? ____ YES ____ NO
- Individual Student Records – protected by FERPA ____ YES ____ NO
- Individual financial information
  - (e.g. credit card and bank account numbers) ____ YES ____ NO
- Other personally identifiable information (PII)
  - (e.g. Social Security Numbers or birth dates) ____ YES ____ NO
- Proprietary Information
  - (e.g. intellectual property or trade secrets) ____ YES ____ NO

☐ Restricted Information: data that is not regulated but for a business purpose is considered protected either by contract or best practice (this includes research data) ____ YES ____ NO

IF ANY OF THE ABOVE ARE "YES", CONTINUE WITH THESE QUESTIONS….

Where is the above information stored and how is it protected?

_____

_____

Do you physically move this information to other locations (such as home or another office)? When discussing this question you should determine if your employee's duties require transporting data and what security measures the employee uses to protect the information while in transit.

- Do you transport data? ____ YES ____ NO
- Describe how you protect this data

  _____

Have you authorized this employee to transport data? ____ YES ____ NO

Discussion Tool for Chairs and Directors
Annual Review of the Privacy, Confidentiality and Information Security Agreement (PCISA)

Do you use University-owned devices for your work? When discussing this question you should identify all the devices that your employee uses (desktop computer, lap top computer, tablet, cell phone, etc.)

- Are your devices password protected and encrypted? ____ YES ____ NO
- If the answer is no, please explain: _____

Do you access, use or store any confidential UW Medicine information on your personal devices? When discussing this question you should identify all the personally owned devices that are used for work.

- What, if any, personally owned devices are used for work?
  _____
- Are all of your devices password protected and encrypted? ____ YES ____ NO
  If you answered no, please explain: _____
- If you need to access confidential UW Medicine information off-site, do you use VPN or CITRIX access? ____ YES ____ NO
  If you answered no, please explain: _____

Are there any areas of concern that you have surrounding UW Medicine's Privacy, Confidentiality or Security requirements? Please explain:

_____
_____

Notes: