

Risk Assessment FAQ

Why must I do this?

HIPAA requires units of the UW-Madison Health Care Component (HCC) to conduct a risk assessment. Completing a risk assessment will give you a general idea of where your strengths and weaknesses lie, with respect to HIPAA requirements.

What must I evaluate?

HIPAA groups standards into three categories of safeguards: technical, physical, and administrative. Therefore, for any system, computer, or network in which PHI is stored or used, you must evaluate the technical safeguards used to electronically protect it (such as encryption, password, access controls, etc.), the physical location of the machines (adequate building security, locks, etc.), and the administrative policies used to guide users of PHI.

How do I really know if HIPAA applies to me or not?

If you are not sure whether HIPAA affects your department or not, you should contact the campus HIPAA Security Officer to discuss your particular situation.

How much time will I spend doing a risk assessment?

When the Risk Assessment Subcommittee evaluated the spreadsheet, it took 3-4 hours to complete the spreadsheet at the test site. Your actual time may be more or less, depending on the size of the department, the number of assets, or other factors. It is probably more important to focus on completeness and thoroughness rather than time spent.

Why use a spreadsheet? Can you not just give us a checklist?

The Risk Assessment Subcommittee designed the spreadsheet to color-code cells based on the grade entered. Using the color codes, one can easily spot areas that one must address. The spreadsheet also helps organize and list the various technical assets, building/locations, and units or subunits that may use or store PHI. You must evaluate each asset, location, and administrative subunit separately.

Why are some columns gray and others white?

Some HIPAA specifications are required. You must address these areas. They appear as gray columns for easy visual identification. The white columns represent items that HIPAA considers "addressable."

Can you give me some guideline(s) to use for assigning a letter grade?

The spreadsheet includes sections that reference the particular HIPAA standards and implementation specifications. That section also lists possible grading scales for required specifications. You can use these scales as a guideline, or you may use another scale that means more to your department with respect to HIPAA.

Can I ignore the "addressable" specifications? The "addressable" specifications have no grading scale.

No. If you can easily identify that you have already implemented the specification you can give yourself an "A". Otherwise, you may want to give yourself a score of "D" or "F" in those areas, and then revisit them once you have dealt with the required issues. HIPAA requires that you completely document your reasoning as to why you feel an "addressable" issue is not reasonable or if you can implement an alternative that still meets the standard. When you revisit them, you may want to document your own grading scale for "addressable" specifications.

How do I evaluate my department's policies? I am not an administrator.

You should not complete the Risk Assessment as an individual. We suggest that a team of 3-4 people complete the Risk Assessment. One suggestion is that someone from IT, another from the department business office, and another from the department management or administrative area be members of this team. You should consult with your HIPAA Security Coordinator to see if specific department policies, procedures, and practices are compliant with HIPAA requirements. Security Coordinators should consult with the campus HIPAA Security Officer.

The sheet that lists the technical assets seems to be missing some of the Administrative specifications. What gives?

Some of the Administrative specifications do not apply to individual technical assets. The Risk Assessment Subcommittee excluded those specifications from the Technical Assets sheet.

Why do I have to evaluate Physical (or Administrative) standards on both the Technical Asset page and the Physical Site (or Administrative Subunit) page?

There is some overlap in terms of what you must evaluate. Physical assessment can apply to physical locations (buildings or rooms), and can apply to individual technical assets. For example, you may have a physical safeguard (a username/password or biometric device) that determines who may use an individual computer. You would also have to evaluate the safeguard(s) that determine who has access to the room containing that computer.

I have dozens of workstations and network devices that I could list as a "technical asset." Must I list each one individually?

If you use the same (or very similar) safeguards on each device, or if they all have a similar configuration, you could evaluate them all as a group and simply enter the group as one technical asset. For example, if you have 15 faculty workstations that use or store PHI, and they all have the same or similar configuration, you could lump all 15 workstations into a group called "Faculty Workstation." You could then enter that group as a single technical asset.

I am not sure what each specification means. Where can I go for help?

The spreadsheet contains HIPAA definitions for each specification. Use that as a starting point, and try to evaluate it with respect to HIPAA for your department. Please contact your HIPAA Security Coordinator. Security Coordinators should contact the campus HIPAA Security Officer.

If I have questions about the Risk Assessment, whom do I contact?

You should contact your HIPAA Security Coordinator. Security Coordinators should contact the campus HIPAA Security Officer.

When must I complete this and to whom does it go?

You should complete the risk assessment as soon as possible, because the risk assessment is a prerequisite for preparation of a migration plan for each unit of the HCC. The migration plan is due by October 14th, or as specified by the HIPAA Security Officer. The risk assessment is also a separate deliverable. If you are not a HIPAA Security Coordinator, send the completed risk assessment to your Security Coordinator no later than October 1st, or as specified by your Security Coordinator. Security Coordinators need to send the completed risk assessment(s) for their unit to the campus HIPAA Security Officer no later than October 14th, or as specified by the Security Officer.