

What is your Research Environment?

o **Standalone Workstation:** You plan to use MHAS restricted data on a computer/workstation that is **physically isolated (air gap)** from the outside world. *[Go to page 3]*

Note: This is a recommended solution; restricted data plans using this approach have a high likelihood of immediate approval.

o **Standalone Network:** You plan to use MHAS restricted data on workstation(s), and server(s) linked to a network that is **physically isolated (air gap)** from the outside world. *[Go to page 5]*

Note: This is a recommended solution; restricted data plans using this approach have a high likelihood of immediate approval.

o **Networked Workstation OR Workstation-Server:** You plan to use MHAS Restricted data on a computer/workstation that is **connected** to your campus or enterprise network. Restricted data will be stored, processed and analyzed on local workstation(s), remote server(s) or both. *[Go to page 8]*

*Note: This is **not** a recommended solution; restricted data plans using this approach will require special technical and procedural evaluation, which may delay approval.*

Work site requirement: We require that the work environment of MHAS Restricted Data users be a secure office or workspace owned by the signing institution. If the workspace is shared, then all occupants must sign the Restricted Data Agreement.

Restricted Data Investigator Name	Title	Institution
IT Department Contact Name	Title	Telephone
IT Contact Signature	Date	

[Page intentionally left blank]

Standalone Workstation (Recommended Solution)

Workstation	Workstation Location (street address, building, office number)	
	Operating system (check one)	<input type="radio"/> Windows 7 Professional/Enterprise/Ultimate <input type="radio"/> Windows XP Professional (Service Pack 3) <input type="radio"/> Macintosh OS X (10.4 and above) <input type="radio"/> Unix family (specify): _____ <input type="radio"/> Other (specify): _____
	Workstation Specifications	Please describe (make/model, form factor): _____
	<input type="radio"/> Yes <input type="radio"/> No	Are all external network connections to the workstation disabled? If the answer to this question is NO, you should complete the Networked Workstation/Workstation Server section.
	<input type="radio"/> Yes* <input type="radio"/> No	Will a laptop be used as the workstation? If yes, provide research justification (this solution is strongly discouraged). You should also explain in detail how wireless connectivity will be disabled. Use the space provided at the end of this section.
	<input type="radio"/> Yes <input type="radio"/> No*	Is workstation login access limited to person(s) specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
	<input type="radio"/> Yes <input type="radio"/> No*	Is the workstation stored in locked office accessible only to the persons specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
	<input type="radio"/> Yes <input type="radio"/> No*	Is the workstation monitor positioned to prevent unauthorized viewing?
	<input type="radio"/> Yes <input type="radio"/> No*	Is physical protection provided for workstation hardware (e.g., BIOS password, locked CPU box)? Describe: _____
	<input type="radio"/> Yes* <input type="radio"/> No	Will removable media be used for storage of restricted data? If yes , in the space provided at the end of this section state: (1) where the removable media to be used will be physically located, (2) how physical access to them is to be restricted and (3) how access to the contents will be controlled.
<input type="radio"/> Yes <input type="radio"/> No*	Is a procedure in place to allow secure updating of workstation operating system and applications software? Describe: _____	
<input type="radio"/> Yes <input type="radio"/> No*	Is anti-virus software installed on the workstation? Describe: _____	

Encryption	o Yes o No*	Is strong encryption (e.g., Bitlocker, Windows Encrypting File System, PGP) installed and in use on the workstation? Describe: _____
	o Yes o No*	Are restricted data files kept in encrypted form when not in use? Describe: _____
Backups	o Yes* o No	Will backups be performed on restricted data files stored on this workstation? If yes, describe the physical and/or software methods to be used. _____ _____
	o Yes o No*	Will restricted data media received from MHAS be stored in a secure location?
Printed Output	o Yes o No*	Are procedures in use to minimize the printing of restricted data elements?
	o Yes o No*	If a local printer is used for printed output is it located in the same locked office as the standalone workstation?

Use this space for explanatory information concerning starred (*) items:

Standalone Network (Recommended Solution)

Workstation (Specify this information for each device)	Workstation Location (street address, building, office number)	
	Operating system (check one)	<input type="radio"/> Windows 7 Professional/Enterprise/Ultimate <input type="radio"/> Windows XP Professional (Service Pack 3) <input type="radio"/> Macintosh OS X (10.4 and above) <input type="radio"/> Unix family (specify): _____ <input type="radio"/> Other (specify): _____
	Workstation Specifications	Please describe (make/model, form factor):
	<input type="radio"/> Yes* <input type="radio"/> No	Will a laptop be used as the workstation? If yes, provide research justification (this solution is strongly discouraged). You should also explain in detail how wireless connectivity will be disabled. Use the space provided at the end of this section.
	<input type="radio"/> Yes <input type="radio"/> No*	Is workstation login access limited to person(s) specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
	<input type="radio"/> Yes <input type="radio"/> No*	Is the workstation stored in locked office accessible only to the persons specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
	<input type="radio"/> Yes <input type="radio"/> No*	Is the workstation monitor positioned to prevent unauthorized viewing?
<input type="radio"/> Yes <input type="radio"/> No*	Is physical protection provided for workstation hardware (e.g., BIOS password, locked CPU box)? Describe: _____ _____	
<input type="radio"/> Yes <input type="radio"/> No*	Is anti-virus software installed on the workstation? Describe: _____ _____	
Network	<input type="radio"/> Yes <input type="radio"/> No*	Is access to MHAS restricted data resources on the network limited to the person(s) specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
	<input type="radio"/> Yes <input type="radio"/> No*	When not in maintenance mode, is the network isolated (no physical connection of any kind, wired or wireless, to any external device) from all forms of public/Internet access? If the answer to this question is NO, you should complete the <i>Networked Workstation/Workstation-Server</i> section.
	<input type="radio"/> Yes <input type="radio"/> No*	Is physical security (locked rooms, locked cabinets and/or storage closets) provided for all network components?

Server	Operating System	
	Server Location (street address, office number)	_____ _____
	o Yes o No*	Are procedures in place to allow secure updating of operating system, applications software and/or firmware for server(s), workstations and network devices? Describe: _____ _____
Encryption	o Yes o No*	Is strong encryption (e.g., Bitlocker, Windows Encrypting File System, PGP) installed and in use on server(s) and when necessary, on workstations? Describe: _____ _____
	o Yes o No*	Are restricted data files kept in encrypted form when not in use?
Backups	o Yes* o No	Will removable media be used for storage of restricted data? If yes, in the space provided at the end of this section state: (1) where the removable media to be used will be physically located, (2) how physical access to them is to be restricted and (3) how access to the contents will be controlled.
	o Yes o No*	Are restricted data files encrypted before backup or transfer to off-line storage?
	o Yes o No*	Are backup media containing restricted data files clearly labeled as such and kept in a secure storage area?
Printed Output	o Yes o No*	Are procedures in use to minimize the printing of restricted data elements?
	o Yes o No*	If a local printer is used for printed output is it located in the same locked office as the workstation?
	o Yes o No*	Are private network printers located in a secure area accessible only to authorized users?

Use this space for explanatory information concerning starred (*) items:

Networked Workstation OR Workstation/Client-Server (Not Recommended)

Workstation (Specify this information for each device)	Workstation Location (street address, building, office number)	
	Operating system (check one)	<input type="radio"/> Windows 7 Professional/Enterprise/Ultimate <input type="radio"/> Windows XP Professional (Service Pack 3) <input type="radio"/> Macintosh OS X (10.4 and above) <input type="radio"/> Unix family (specify): _____ <input type="radio"/> Other (specify): _____
	Workstation Specifications	Please describe (make/model, form factor):
	<input type="radio"/> Yes* <input type="radio"/> No	Will a laptop be used as the workstation? If yes, provide research justification (this solution is strongly discouraged). You should also explain in detail how wireless connectivity will be disabled. Use the space provided at the end of this section.
	<input type="radio"/> Yes <input type="radio"/> No*	Is workstation login access limited to person(s) specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
	<input type="radio"/> Yes <input type="radio"/> No*	Are all forms of access to this workstation (including VPN and/or remote desktop connections) from outside or inside the institutional network disallowed?
	<input type="radio"/> Yes <input type="radio"/> No*	Have restricted data users received instruction on avoidance and mitigation of workstation security risks in a public network environment? Describe: _____
	<input type="radio"/> Yes <input type="radio"/> No*	Is the workstation stored in locked office accessible only to the persons specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
	<input type="radio"/> Yes <input type="radio"/> No*	Is the workstation monitor positioned to prevent unauthorized viewing?
	<input type="radio"/> Yes <input type="radio"/> No*	Is physical protection provided for workstation hardware (e.g., BIOS password, locked CPU box)? Describe: _____
	<input type="radio"/> Yes <input type="radio"/> No*	Are Web browsers configured to minimize security risks (example: current version of Firefox with Adblock Plus, NoScript and BetterPrivacy add-ons installed)? Describe: _____
	<input type="radio"/> Yes <input type="radio"/> No*	Is access to social network applications such as Facebook, Twitter, Google+, LinkedIn disabled while MHAS restricted data products are in use?
	<input type="radio"/> Yes <input type="radio"/> No*	Is anti-virus software installed on the workstation? Describe: _____

Encryption	<input type="radio"/> Yes <input type="radio"/> No*	Is strong encryption (e.g., Bitlocker, Windows Encrypting File System, PGP) installed and in use on server(s) and when necessary, on workstations? Describe: _____ _____
	<input type="radio"/> Yes <input type="radio"/> No*	Are restricted data files kept in encrypted form when not in use?
Network	<input type="radio"/> Yes <input type="radio"/> No*	Are “best practice” system management procedures in place to control user and group access to network resources and maintain workstation and network security?
	<input type="radio"/> Yes <input type="radio"/> No*	Are procedures in place to allow secure updating of operating system, applications software and/or firmware for server(s), workstations and network devices? Describe: _____ _____
	<input type="radio"/> Yes <input type="radio"/> No*	Will a VPN be used to secure communications between workstation(s) and server(s)? Describe: _____ _____
	<input type="radio"/> Yes <input type="radio"/> No*	Are intrusion detection/prevention systems installed and maintained for the server(s), workstation(s) and other devices attached to this network segment? Describe: _____ _____
	<input type="radio"/> Yes <input type="radio"/> No*	Is firewall protection provided for the network segment(s) where restricted data client and server(s) are located? Describe: _____ _____
	<input type="radio"/> Yes <input type="radio"/> No*	Is network access to MHAS restricted data products limited to person(s) specified in the <i>Restricted Data Agreement</i> and/or <i>Supplemental Agreement</i> ?
Server	Operating System	
	Server Location (street address, office number)	
<input type="radio"/> Yes <input type="radio"/> No*	Are VPN and/or remote desktop connections from outside the institutional network to this server disallowed?	
Backups	<input type="radio"/> Yes* <input type="radio"/> No	Will removable media be used for storage of restricted data? If yes , in the space provided at the end of this section state: (1) where the removable media to be used will be physically located, (2) how physical access to them is to be restricted and (3) how access to the contents will be controlled.
	<input type="radio"/> Yes <input type="radio"/> No*	Are restricted data files encrypted before backup or transfer to off-line storage?
	<input type="radio"/> Yes <input type="radio"/> No*	Are backup media containing restricted data files clearly labeled as such and kept in a secure storage area?
Printed output	<input type="radio"/> Yes <input type="radio"/> No*	Are procedures in use to minimize the printing of restricted data elements?
	<input type="radio"/> Yes <input type="radio"/> No*	If a local printer will be used for printed output, is it located in the same locked office as the workstation?
	<input type="radio"/> Yes <input type="radio"/> No	Will printouts be sent to network printers? If yes, describe how security of printout content will be maintained:

Use this space for explanatory information concerning starred (*) items:
