Alternative work arrangement information & privacy home checklist

Employees must complete and return to their Manager prior to starting an alternate workplace arrangement (AWA).

Audit Date (YYYY-MMM-DD)	
Employee Name:	
Employee Position:	
Manager Name:	
Manager Position:	

Privacy Process Requirements	**Compliance Status**			
	Yes	**No**	**N/A**	**Action/Comments**
Physical Security				
1. Is the home work area secure and dedicated to the use of you, the Covenant Health employee, at all times?				
2. If the home work area is not dedicated to your use at all times, is the work area private and secure from physical entry or overhearing confidential information by unauthorized individuals?				
3. Will phone discussions be conducted in a place and manner to reduce the potential for unintentional disclosure?				
4. Is work area a separate and secure area that can be controlled by lock and key?				
5. Will the computer equipment used to access AHS/Covenant information systems be physically secured via locking				
6. Will computer screens in work locations be positioned so as not to be visible to others?				
7. Will computer areas, desks, bulletin boards be free of written passwords, usernames, and log in instructions?				
Computer and Mobile Device				
8. Will the computer equipment used to connect to the AHS/Covenant network be dedicated to the use of the individual working in the home setting?				
9. Will AHS/Covenant mobile computing devices used (e.g. memory sticks, smart phones) be stored in a secure location				
10. If mobile devices are in use, are they used in compliance with AHS and COV policies?				
Information Security				
11. Will all information being accessed be stored on the secure AHS network?				

12. All work related email communication must be conducted via the AHS email system. Will email be sent or received via any other method? (e.g. Shawmail, @home, gmail) If so, why?				
	Yes	**No**	**N/A**	**Action/Comments**
13. Will any confidential information be stored locally on any AHS computer or mobile device? If so, why?				
14. Will any confidential information be stored locally on your personal computer or mobile device? If so, why?				
Printers				
15. Will there be a printer connected to the computer via remotely at a Covenant site? If yes, who will be gathering printed material at the Covenant site for the employee?				
Fax/Scanning				
16. Is faxing/scanning a requirement of the employee's role?				
17. Will faxes/scanning be completed directly on an AHS/Covenant computer?				
18. Will electronic fax cover sheets be used for each fax? Is there "autodial" capacity?				
Manager/Supervisor's Administrative & Privacy Considerations				
19. Has the employee read and agreed to all Information Management Policies? Ie. Information Privacy Breach or Information System Security Incident Response (July 11, 2014) X-40, Information Technology Acceptable Use and Safeguards (July 11, 2014) X-50				
20. Has the employee completed the Information & Privacy Training?				
21. Has the employee read and signed current Covenant Health Confidentiality agreement and IT User Agreements?				
22. Is employee is aware of how to report a privacy or security breach? Are they able to verbalize what to do if a breach occurs (e.g. a misdirected fax, a missing chart, information accessed or overheard by an unauthorized person)?				
Completed by **Signature**				
Employee Name	**Date** (YYYY-MMM-DD)			
Manager Name	**Date** (YYYY-MMM-DD)			