INFORMATION CONFIDENTIALITY AND SECURITY AGREEMENT (ICSA)

POLICY ACKNOWLDGEMENT AND COMPLIANCE ATTESTATION

INTRODUCTION TO RESOURCE SECURITY

Information security of all Ardent Information Resources is of the utmost importance to Ardent, including the protection of Ardent data, applications, systems, and network resources from accidental, negligent, or deliberate misuse through disclosure, alteration, or destruction.

Resources include all Ardent-owned or provided:

- electronic data and documentation;
- online screen transactions;
- software applications;
- data set files and databases residing in any media, such as tape, disk, CD-Rom, DVD;
- processing systems to include servers, PCs, workstations, and printers; and
- network resources

It is every user's responsibility to guard against unauthorized use, access to, destruction or disclosure of these as Ardent Information Resources. Users should refer to Ardent's Document Retention Policy, CD-011 for specific document retention (including electronic data) requirements. Every user is responsible for reasonable protection of all information and Information Resources.

Ardent stores, processes, and disseminates large amounts of critical information. It is imperative to ensure the integrity, accuracy, availability, and confidentiality of the Information Resources through the use of industry standard security controls.

USER RESPONSIBILITIES

Each user of Ardent Information Resources is responsible for safeguarding the confidentiality and integrity of Information Resources to which he or she has access. This acknowledgment form and all Information Security policies apply to all users of the Ardent computer systems, including employees, partners, vendors, contractors, and other individuals who have been granted access authority to Ardent Information Resources.

If you have a User ID, you are responsible for the confidentiality of the password, and for any action performed with your User ID.

The following guidelines must be adhered to:

1. Your User ID and password are to remain strictly confidential; do not lend them out or share them with others. You and/or your employer are personally accountable for all actions that occur under your User ID.
2. Upon initial login, change your password and select an alphanumeric password having upper and lower case letters, numbers, and special characters and one that would be easily "guessed." Pass phrases are the most acceptable, in which a phrase is used in combination with numbers. Do not use repeating characters. Do not use obvious passwords such as your name, your spouse's, children's or pet's names, days of the week, names of months, your User ID, birthday, phone, Social Security number, or terms such as "none", "login" or "password". Make sure your password is a minimum of seven characters in length and that it is changed a minimum of every 90 days (special passwords granting access at administrator or supervisor level must be changed at least every 30 days).
3. Memorize your password instead of writing it down and do not store it in programmable function keys.
4. Log out or lock your terminal when leaving it, even for a short period of time. Be sure to log out when you leave for lunch or meetings.
5. Keep documents, diskettes, and copies of files containing sensitive data in a secure cabinet, desk, or room, and dispose of them properly when no longer needed. (See Ardent's Document Retention Policy, CD-011 for more information on proper disposal of records and InfoSec P040 Electronic Media_Equip Disposal_Removal Standards for instructions on Media and Equipment disposal). Reformat reusable diskettes containing sensitive data before releasing them for reuse.
6. Ensure that your data and transactions are protected against unauthorized use.
7. If you think your User ID or password has been compromised in any way, immediately change your password, and notify your supervisor of the Facility Security Coordinator for your business area.
8. Report all suspicious activity, breaches in security, and practices not conducive to good data security to your supervisor or Local Security Coordinator for your business function.
9. Protect the confidentiality of sensitive data when viewing it online, and do not use public computers to access any such information.
10. Do not disclose any portion of a patient's record except as authorized by applicable regulations. (See Ardent's HIPAA Policies for more detailed information).
11. Information Resources are to be used only in accordance with the Ardent Policy on Ethics and Compliance (Personal Use of Company Resources). Use for anything other than that for which you are authorized is considered misuse.
12. Users should take precautions to prevent the introduction of software viruses into the Computer Resources. Games, files downloaded from bulletin boards and the Internet, and software brought from home increase the risk of loss due to viruses and other malicious software on the network and may not be installed without the express authorized of Ardent's Chief Information Officer.
13. Use only authorized and licensed software on Ardent systems. Complete compliance with the U.S. Copyright Act, 17 U.S.C. §§ 101 – 810 is mandatory. NO EXCEPTIONS.

SECURITY POLICY ACKNOWLEDGMENT AND AGREEMENT

An executed copy of this Agreement must be submitted by all users of the Computer Resources to include Ardent employees, employees of temporary employment agencies, vendors business partners, and contractor personnel and functional units regardless of geographic location. The original signed copy is to be retained by Ardent in the employee's personnel file. Non-employee signed forms are to be retained by the hiring manager. Modifications to the terms and conditions of this Agreement will not be accepted by the CIO.

Internet activity, opened e-mail, and processing systems activity, transactions, and files that are present on or use Ardent-owned or provided Computer Resources are subject to monitoring to prevent abuse, misuse, or for any other legitimate business reason.

COMPLIANCE TERMS

Signing this form constitutes acknowledgment by you of your responsibility to guard against unauthorized use or disclosure of Computer Resources or information, and agreement that you will comply with all of the security policies and rules listed in this acknowledgment form and with all associated security documents. Failure to comply with security policies, rules, and associated documents may result in disciplinary action, up to and possibly including termination from Ardent in the case of employees and the termination or cancellation of agreements in the case of physicians or hospital staff, consultants, contractors, or vendors.

Employee/Physician/Consultant/Contractor/Vendor Signature	Company/Facility	Date
Employee/Physician/Consultant/Contractor/Vendor Printed Name		

Ardent[SM]
HEALTH SERVICES

Name of School _____ Name of Instructor_____

CONFIDENTIALITY ACKNOWLEDGMENT

Through my association with _____(facility) as student, or approved observer, I understand that patient information in any form (paper, electronic, oral, etc) is protected by law and that breaches of patient confidentiality can have severe ramifications up to and including termination of my relationship with _____(facility) as well as possible civil and criminal penalties. I will only access, use or disclose the minimum amount of patient information that I am authorized to access, use or disclose and that is necessary to carry out my assigned duties. I will not improperly divulge any information which comes to me through the carrying out of my assigned duties, program assignment or observation.

This includes but is not limited to:

- I will not discuss information pertaining to any patient with anyone (even my own family) who is not directly working with said patient.
- I will not discuss any patient information in any place where it can be overheard by anyone who is not authorized to have this information.
- I will not mention any patient's name or disclose directly or indirectly that any person is a patient except to those authorized to have this information.
- I will not describe any behavior, which I have observed or learned about through association with this Facility, except to those authorized to have this information.
- I will not contact any individual or agency outside this Facility to get personal information about an individual patient unless an Authorization has been signed by the patient or by someone who has been legally authorized by the patient to release information.
- I will not use confidential _____ (facility) business related information in any manner not required by my job or disclose it to anyone not authorized to have or know it.
- I will not access information concerning any patient in whose care I am not directly involved other than as established by my Job Description.
- I understand my responsibility to take action when faced with a privacy concern or become aware of a potential violation of our privacy policies and standards. This includes:
  - ▶ **RECOGNIZE** the concern and nature of the situation
  - ▶ **RESPOND** appropriately
  - ▶ **REPORT** the issue to someone who can assist in resolving the matter

I understand that my agreement to maintain the confidentiality of patient information is a condition of my continued relationship with Ardent Health System.

With my signature, I indicate I have read and understand this Acknowledgment.

Printed Name_____

Signature_____ Date_____