Purpose:

Maintaining the security and confidentiality of information is a paramount concern of Carle Clinic Association and its employees and patients. Carle Clinic’s concern in this regard is heightened by the various technology resources provided to its employees to facilitate the creation and communication of business-related information in the most effective and efficient manner possible. Because more information may be transmitted in less time and with less formality, we all must put more effort to maintaining confidentiality, accuracy, security and control of the information.

We also must ensure the ethical, professional and judicious use of technology resources. Proper use demonstrates respect for patient confidentiality, security mechanisms, data ownership, intellectual property, and a harassment-free workplace. This is especially true because electronic communications tend to be more immediate and informal than written communications and because passwords and deletion functions create the illusion of privacy, control and confidentiality. Whether intentional or due to carelessness, the release of confidential patient information is unethical and may result in litigation against Carle Clinic and its employees.

Relatedly, although the Internet can be a valuable information resource for legitimate business, research and information sharing, it presents a significant opportunity for abuse, lost productivity and potential liability.

In light of these concerns, Carle Clinic has developed this Policy, which establishes the parameters for technology resources usage and serves to enhance employee awareness of our obligation to hold patient information confidential. This Policy supplements all existing federal, state, local, and Carle Clinic laws, regulations, agreements, and contracts, which currently apply to information confidentiality and technology resources. All persons who are authorized to access confidential information and use technology resources must comply with this Policy. Users who do not comply with this Policy are subject to assessment of line usage payment (if appropriate), the revocation of their access to technology resources and disciplinary action up to and including discharge. (See Clinic Policy #1203 for more information about the Disciplinary process.)

Scope:

This Policy applies to all Carle Clinic employees and other persons who are authorized to use Carle Clinic technology resources, including certain consultants, contractors, vendors, students, volunteers and residents ("users"). This Policy applies to the following forms of technology resources and information created by their use, including but not limited to (1) computers (including desktop, portable, servers, mainframes, local area networks, wide area networks, printers, software and removable storage media (e.g., floppy disks, CD-ROMs, hard disks)); (2) electronic mail ("e-mail"), including attachments; and (3) the Internet and Intranet.

For purposes of this Policy, "confidential information" is all information, whether oral or recorded in any form or medium, obtained in the course of providing medical care or treatment which identifies or can be associated with the identity of a patient and/or the nature of a patient’s medical care and treatment. See also Clinic Policy #4201. Confidential information also includes employee personnel information such as applications, evaluations, salary, letters of warning, etc. See also Clinic Policy #1102 http://cweb.carle.com/ClinicPersonnel/Policies/302.htm.
Confidential information includes all such information entered, created, received, stored or transmitted via Carle Clinic’s computer network and accessible through computer terminals, PCs or printers by either visual display or hard copy output.

The Information Technology Department ("the ITD") will administer user authorization. Managers must timely inform the ITD of all staffing changes (e.g., new hires, terminations, transfers) that require a change in access to Carle Clinic technology resources.

**Statement of Policy:**

1. **ANY UNAUTHORIZED ACCESS OR USE OF THE CARLE NETWORK IS STRICTLY PROHIBITED.**
   
   A. The Carle computer network, including all applications and all information entered, created, received, stored or transmitted herein, is the property of Carle Clinic Association. All information entered, created, received, stored or transmitted on this system are the property of Carle Clinic Association and may be accessed by authorized personnel. Users should not have any expectation of privacy with regard to the entry, creation, transmission, receipt, or storage of information via the network.

2. **Other Than Occasional Personal Use, Carle Technology Resources May Be Used Only For Legitimate, Business-Related Reasons**
   
   A. Other than occasional personal use, Carle technology resources may be used only for legitimate business-related reasons. Occasional personal use means minimal and infrequent use that does not interfere with Carle business or the availability of technology resources. All use of Carle technology resources (including personal use) is subject to this Policy.

   B. Carle technology resources may not be used for personal commercial or profit-generating activities unrelated to Carle’s business without express management approval. All information that is entered, created, received, stored or transmitted via Carle technology resources, including all e-mail messages, are and will remain Carle property. Information generated in the context of Carle business may neither be used for any purpose unrelated to Carle business nor sold, transmitted, conveyed or communicated in any way to anyone outside of Carle without express management authorization.

3. **No Expectation of Privacy**
   
   A. Users should have no expectation of privacy in connection with the entry, creation, transmission, receipt, or storage of information via Carle technology resources. Users waive any right to privacy in information entered, created, received, stored or transmitted via Carle technology resources, and consent to access and disclosure of such information by authorized Carle personnel.

   B. As with all other Carle property, Carle technology resources and all information entered, created, transmitted, received or stored via Carle technology resources is subject to inspection, search and disclosure without advance notice by persons designated or acting at the direction of the Assoc. Admin. of ITD or Chief Administrative Officer, or as may be required by law or as necessary to ensure the efficient and proper administration and operation of Carle’s technology resources. For example, authorized persons may inspect, search and disclose such information to investigate theft, disclosure of confidential business or proprietary information, personal abuse of the system, or to monitor workflow or productivity. Because Carle is sensitive to employee concerns, it will make every effort to ensure that all such inspections are conducted professionally and ethically. Users, however, must recognize that authorized persons have the ability to track and monitor all information sent internally and externally to Carle via technology resources.

   C. All passwords and security used in connection with Carle technology resources are Carle property and must be available to Carle. Users should understand that their use of passwords does not preclude authorized persons to access Carle technology resources. Passwords may not be shared between Carle employees nor may unauthorized individuals use them to obtain access to information. Carle reserves the right to assign and/or change passwords and personal codes for voice mail, E-mail, and computer applications.
4. The Creation Or Transmission Of Any Information That May Be Construed To Violate Carle's Harassment-Free Workplace Policy Or Equal Employment Opportunity Policy Is Strictly Prohibited

   A. Users are strictly prohibited from using Carle's technology resources in any way that may be offensive to others. This prohibition includes, for example, the transmission of sexually explicit or obscene messages or cartoons, ethnic or racial slurs, or anything that may be construed as unlawful harassment or disparagement based on race, color, religion, sex, national origin, age, disability, ancestry, sexual orientation, marital status, parental status, source of income, military discharge status, or any other status protected by law. Relatedly, users may not use technology resources to transmit critical or derogatory statements regarding individual employees, patients, consultants, contractors, vendors, students, volunteers or residents. Users violating these prohibitions may be subject to disciplinary action, up to and including termination.

5. Use Of Carle Technology Resources Is Subject to Carle’s No-Solicitation/No-Distribution Policy

   A. Carle policy strictly forbids individual employees from soliciting, during their working time or the working time of the employee being solicited, any other individual to support any individual or organization without the approval of administration. It also forbids individual employees from distributing any literature on behalf of any individual or organization on Carle property unless approved by administration. This includes the distribution of chain letters of all kinds. Use of Carle technology resources, including e-mail, must be consistent with this policy -- Carle technology resources may not be used for such prohibited solicitation or distribution purposes.

6. Intellectual Property Laws And Computer Standards

   A. Users may not violate any copyright, patent or other intellectual property law, including restricted software laws. Accordingly, unless permission has been expressly and officially provided, users may not post or download any information protected by copyright or patent law. If copyright, patent or other ownership status is unknown, users may not post, upload, download or otherwise use any information, content, software or other property and should consult the network administrator with any inquiries.

   B. Although Carle purchases and licenses various computer software for business purposes, unless otherwise authorized by the software developer, Carle does not have the right to reproduce such software for use on more than one computer. Users thus may only use software according to the software license agreement and may not duplicate software and its related documentation in violation of that agreement. Relatedly, software purchased and licensed for personal use that does not have a purpose related to Carle’s business, its installation on Carle computers is strongly discouraged. To establish uniform standards and reduce costs, Carle will publish on Cweb a list of computer hardware and software that the ITD is authorized to install, maintain and support. The ITD and/or the Architectural Review Committee will evaluate user requests to change the list. Carle may, at any time, conduct an audit or interrogation of computers for installed software and related printed material that is not included on a then-current inventory of Carle-authorized software. All personal, non-work related unauthorized software that disrupts normal use of Carle’s Information Technology system will be removed and destroyed. (Also see non-standard support policy.)

7. Viruses

   A. All Carle technology resources must be protected from accidental destruction or deliberate attempts at sabotage by computer viruses. Users thus may not willfully introduce virus-infected files or media into Carle technology resources. Users must make all reasonable efforts to ensure that all files accessed or collected are virus-free, should minimize downloading information from the Internet and via e-mail and should not download information from unfamiliar Internet sites. Users should use discretion when receiving e-mail from unknown sources, especially where the e-mail contains attachments. Prior to placing any file on the Carle network, Users must scan for viruses using up-to-date, approved virus-scanning software. See Clinic Policy #424, Carle Computer Virus Protection Policy for more information.

8. ITD Work On Privately-Owned Technology Resources
A. Users must password-protect all material of a personal or offensive nature before seeking assistance from the ITD to work on privately-owned technology resources (e.g., to install or repair programs that will allow the user's personal computer to interface with the Carle network). Relatedly, (pursuant to item 9) users must encrypt all material of a personal or offensive nature to prevent inadvertent access by the ITD.

9. Confidential Information

A. Users must take every measure to ensure that confidential information that is entered, created, received, stored or transmitted via technology resources remains confidential. For example, the contents of any record or report may not be released except as is necessary in performing one's job and in accordance to Carle policy (Clinic Policy #4201). Likewise, users must continue to respect the confidentiality of any report containing confidential information while handling, storing, and disposing of these reports in an appropriate manner. Users may not knowingly enter, electronically or otherwise, false or inaccurate information into reports or records.

B. Users are prohibited from searching for, using, sending, posting or otherwise disclosing confidential information outside or within Carle without express management authorization. To this end, users must immediately cancel all bundled mailing lists that are not directly related their professional responsibilities.

C. Users should be aware that although ITD staff, in the performance of their duties, may view personal and confidential material, they must not do so intentionally or otherwise disclose or use what they have seen, except as provided elsewhere in this Policy.

D. The Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA") has added requirements for the privacy and security of Patient Health Information. Clinic Policy #4201 has been created to safeguard the protection of PHI. The two opening paragraphs of the policy purpose are: Our patients' health and medical records are personal in nature. Carle is committed to protecting the confidentiality of the information obtained from patients during the course of their health care, the payment of that health care, and other related operations. Carle Staff and Physicians should be aware of their obligations to hold confidential all protected health information (PHI), and encourage practices that are within the accepted principles and guidelines set forth in Clinic Privacy Policies. Carelessness or thoughtlessness leading to release of information about patients is wrong ethically and may result in litigation against the policy violator and Carle organizations.

10. Password/ID Usage

A. Carle employee computer User IDs and passwords are for sole use of that employee. Carle employees are not to share their computer User IDs and passwords with other individuals or use another individual's User ID. Carle employees must take precautions to safeguards passwords and other privileged information to which they have been given access. Any passwords, verification codes, or electronic signature codes are for their individual use only. They are to regard them as personal identifiers of their computer use, similar to their signature on a document. They are responsible for all actions performed from their computer User ID. Contact the IT Helpdesk immediately if you believe that your User ID is being used without your permission.

11. Paging Policy

A. Paging access is for legitimate business-related and administrative purposes. All pages are recorded and logged. See Carle Clinic's Paging Policy #426.

12. Encryption

A. To ensure continuous access to technology resources, users shall not use personal hardware or software to encrypt information entered, created, received, stored or transmitted via technology resources, except in accordance with Carle's express written permission. (See also item 8.)
13. Internet Use

Like all other technology resources, Carle provides Internet access only for legitimate business-related health care, education, research, outreach, and administrative purposes. The Internet shall not be used for any personal use, including private consulting and commercial enterprises.

A. Internet Access Generally

- Users must obtain written authorization from their department manager to use Carle technology resources to access the Internet. Requests for Internet access must be based on legitimate, business-related reasons. The ITD will terminate any unauthorized connections to the server. Department managers who authorize access to the Internet are responsible for promptly notifying Carle’s network administrator when Internet users terminate, change departments or no longer require Internet access.

- Off-site users who access the Internet via Carle-provided technology resources (e.g., via a Carle-provided laptop computer) shall adhere to all of the same policies that apply to use from within Carle facilities. Users may not permit family members or other non-employees to use Carle-provided technology resources and/or access Carle’s computer systems.

- All requests to access blocked Internet sites must be made, in writing or via e-mail to Carle.internet@carle.com, to the ITD or the Medical Director of Information Technology, and will be evaluated pursuant to an established procedure. Appeals to these decisions can be made to Carle I.T. steering Committee. Appeals of this Steering Committee’s decisions can be made to Carle Clinic Administration or Carle Foundation Administration.

B. External Internet Access

- Users who wish to obtain external access to Carle’s Intranet or Internet access must obtain the prior written approval of their manager and the ITD. When accessing Carle’s Intranet or using Carle’s Internet access, users must do so only through Carle’s authorized dial-in connection. Because Carle wishes to maintain its excellent reputation, it is imperative that all users who have external Internet access adhere to this Policy and all other Carle rules and guidelines, exercise extreme precaution in their representation of Carle and ensure that, absent Carle express management authorization, their Internet communications do not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Carle or any unit of Carle.

C. Internet Sites

- Carle has established two Internet sites -- www.carle-clinic.com and www.healthalliance.org -- to serve as the official sites of Carle and Health Alliance, respectively. These sites have been designated to represent and speak on behalf of Carle to persons outside of the organization. No other sites may be established or purport to represent Carle, or any part thereof, although other Internet sites, with prior approval of the appropriate marketing department, may refer to Carle or Health Alliance and link to their home page or part of the two official sites. The Carle/Health Alliance marketing departments are responsible for monitoring the content of their respective external sites to ensure the consistency and propriety of all displayed information. All requests and inquiries regarding the external sites should be directed to Carle and/or Health Alliance’s marketing departments.

14. Use Of Carle’s Intranet

A. With regard to Carle’s Intranet, departmental managers may ask the Information Systems Department to limit access to their entire site or particularly sensitive material within the site. Because system security turns on the discrete use of IDs and passwords (or lack thereof), users who have access to restricted areas of Carle’s Intranet are responsible for protecting, modifying, and periodically devising unique passwords. It is imperative that users use extreme caution in maintaining ID and/or password confidentiality because intentional or
inadvertent disclosure of IDs and/or passwords could result in substantial liability.

15. Notification Of Policy Violations And Cooperation With Investigations

A. Users must notify their supervisor of violations of this Policy and should endeavor to prevent unauthorized use of or access to information stored or processed within Carle technology resources. Users are expected to cooperate with security investigations related to Carle technology resources and this Policy.

16. E-Mail Retention Policy

A. Several years have passed since the Microsoft Outlook email system was implemented at Carle. During that time, hundreds of thousands of email documents have been sent from and received into the Carle system. While many staff have been diligent in saving and filing only those documents deemed important and necessary for Carle business, many others have allowed a significant volume of non-essential email documents to accumulate. Given the size of the Carle enterprise, the amount of space consumed by email documents quickly becomes very challenging to manage.

B. In order to best utilize Carle resources, a policy on email retention will be instituted on July 1, 2003. The policy will only be directed at email documents contained within the Outlook Inbox, Sent Items, and Deleted Items folders. The policy will be implemented as follows:

C. Email documents older that one year will be automatically deleted from the Inbox, Sent Items, and Deleted Items folders. The deletion process will NOT affect any email documents contained within a personal folder.

D. Email documents to be retained beyond one year will need to be moved to a personal folder. If you have any questions on how to utilize Outlook personal folders, please use the Outlook Help function to review. If you have additional questions on how to best utilize the personal folder feature, contact the Carle Help Desk at 383-4357.

Definitions:

Procedures:

1. Monitoring Guidelines

A. The Information Technology Department should follow the following guidelines to the greatest extent possible in, monitoring, inspecting and searching Carle technology resources and information entered, created, transmitted, received or stored via such resources. These guidelines are based on the Privacy Working Group of the Governmental Information Infrastructure Task Force’s "Principles for Providing and Using Personal Information."

B. "Authorized persons" are those persons who are designated by or acting at the direction of the Director of the Information Technology Department (or as may be required by law or as necessary to ensure the efficient and proper administration and operation of Carle’s technology resources) who monitor, inspect, or search information in connection with the Carle Health Information And Technology Resources Policy and should have an Information Technology Work Request form properly authorized by an Associate Administrator (Clinic) or Vice-president (Foundation). Approval of such "authorized persons" as noted above would come from the Clinic’s CEO, COO, or Medical Director, or from the Foundation’s CEO, Senior Vice-President of Operations or Vice-president of Information Technology. In deciding whether to monitor, inspect or search and in so doing, authorized persons should:

• Assess: (1) why the information is being collected; (2) what the information is expected to be used for; (3) what steps will be taken to protect its confidentiality, integrity, and quality; (4) the consequences of
providing or withholding information.

- Not improperly alter or destroy personal information;
- Ensure that personal information is accurate, timely, complete, and relevant for the purpose for which it is obtained and used; and
- Use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information.

2. Intellectual Property (Copyright and Patent) Laws And Computer Standards

A. To establish uniform standards and reduce costs, the ITD will publish on Cweb a list of computer hardware/software that the ITD is authorized to install, maintain and support. The ITD will compare all new hardware/software purchases and installations to the list and deny all requests to maintain and support unauthorized software/hardware. Users may submit requests to change the list to the Architectural Review Committee and/or the Information Technology Steering Committee according to the attached flowchart. The ITD will review all software/hardware that is interfaced to the Carle network for compliance with the supported network standards.

3. Access To Blocked Internet Sites

A. All requests to access blocked Internet sites must be made, in writing, to the ITD or the Medical Director of Information Technology. Requests will be approved if deemed appropriate and consistent with business necessity. Denied requests may be presented, in writing, to the Information Technology Steering Committee. Requests denied by the Information Technology Steering Committee may be appealed, in writing, to the Carle Clinic Board of Governors. Appeals to the Information Technology Steering Committee and/or the Carle Clinic Board of Governors must include a list of requested sites and examples of each site’s web pages. Requesters who do not have independent access to the blocked sites he or she wishes to access may seek the assistance of ITD staff to obtain this material, the quantity of which must not be excessive.

4. Carle Information Technology Non-Standard Support Policy

A. Carle Information Technology will support all software and hardware identified in the Computer Usage Policy as listed on CWEB. Support of any personal hardware and software on Carle machines will be handled as follows (NO PERSONAL SOFTWARE MAY BE INSTALLED ON THE NETWORK):

B. Personally Installed Software: Personal software should not interfere with Carle software/hardware on the PC. If the installation of personal software causes a problem requiring the assistance of Carle Information Technology staff, the installer will be responsible for reimbursing Carle Clinic at the rate of $50.00 per hour from portal to portal (includes travel time). Carle Information Technology will not be responsible for installing or maintaining personal software of any kind.

C. Games: Games are the responsibility of the installer. If the installation of a game causes a problem requiring the assistance of Carle Information Technology staff, the installer will be responsible for reimbursing Carle Clinic at the rate of $50.00 per hour portal to portal (includes travel time). We will not be responsible for installing or maintaining games of any kind except those installed with an operating system.

D. Home Dial-up: Desktop staff will install and support home dial-up for Carle staff with appropriate authorized work order requests. All others will be billed at the rate of $50.00 per hour. If desktop support staffs are asked to support non-Carle hardware/software, they may do so within reason at the rate of $50.00 per hour.
**Acknowledgement:**

I acknowledge that I have received a copy of Carle’s Health Information and Technology Resources Policy and that I have read and understand the Policy. I understand that Carle technology resources and all information entered, created, received, stored or transmitted by those resources are the property of the Carle. I have no expectation of privacy in connection with the use of Carle technology resources or with the entry, creation, transmission, receipt, or storage of information via Carle technology resources.

I understand that I must comply with all of the provisions of the Policy to have access to and use Carle technology resources. I also understand that if I do not comply with all provisions of the Policy, my access to Carle technology resources may be revoked and I may be subject to disciplinary action up to and including discharge. (See Clinic Policy #1203 [http://cweb.carle.com/ClinicPersonnel/Policies/303.htm](http://cweb.carle.com/ClinicPersonnel/Policies/303.htm) for more information about the Disciplinary process.)

<table>
<thead>
<tr>
<th>Signature Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printed Name</td>
</tr>
</tbody>
</table>

**Attachment(s):**

**References:**

**Signatures**

<table>
<thead>
<tr>
<th>Signature on File in Clinic Administration</th>
</tr>
</thead>
</table>

Michael W. Bukosky  
Executive Vice President, Chief Administrative Officer