Title: Technology Resources Utilization

Policy #: ADM-04

Purpose: Beth Israel Deaconess Medical Center ("BIDMC") has adopted this Technology Resources Policy to ensure uniform and appropriate use of its computer and telecommunication resources (the "Technology Resources," defined below). The rules, obligations, and standards described in this Policy apply to all employees, temporary workers, independent contractors, agents, and other computer or telecommunication users (collectively, the "Users," as defined below), wherever they may be located.

It is every User's duty to use the Technology Resources responsibly and in a professional, ethical, and lawful manner. In addition, every User is responsible for ensuring the security of BIDMC's Technology Resources and its valuable proprietary and confidential information.

Users who become aware of any violation of this policy must immediately report the incident to the Chief Information Officer or his/her designated representative. Violations of this Policy may result in disciplinary action, including possible termination, and potential civil and criminal liability. Use of the Technology Resources is a privilege that may be limited or revoked at any time, with or without cause and without notice, in the sole discretion of BIDMC.

Definitions:

As used in this Policy, certain terms are defined as follows:

"Confidential/Proprietary Information" may include all material, in any form, related to the operation of CareGroup or a controlled subsidiary, including, but not limited to health information, financial information, employee information, proprietary products and product development, marketing and general business strategies, and any information marked "confidential". Specific state and federal laws protect alcohol or substance abuse; sexually transmitted disease; and HIV status information. Access to confidential information is restricted according to this policy and applicable laws and regulations.

"Computer Information" means all information and communications created, received, or stored on or passed through the Technology Resources. Computer Information includes all User files and e-mail.

"Copyrighted Publications" means materials that are subject to protection under the law of copyright. These materials include, but are not limited to, third party software, software manuals, trade articles, textbooks, newspaper and magazine articles, electronic databases, graphics, audio files, pictures, and material available on the Internet. While having a copyright notice and/or a "©" may provide the copyright owner with additional rights, they are not required for copyright protection to apply. Almost every document, whether written or electronic, is subject to copyright protection – whether or not they have a copyright notice. When in doubt, Users should always assume that a document is copyrighted.

"Data/Telecom Network" means the electronic components, wireless frequencies, patch cords, network interface cards, cabling, wall jacks, patch panels, software, routers, switches, extension cabinets, intrusion detection engines, network firewalls, content filters and

other components that are integral to the movement of data, voice, and video signals within the data/telecom environment deployed and managed by BIDMC.

"E-mail" means messages, including instant messages, sent from one person to one or more individuals or groups (or addresses on a distribution list) via electronic media, either through an internal network or over an external network (e.g., the Internet or America Online). Messages may consist of digitized text, graphics, video, voice and/or file attachments.

"Firewall" means a hardware and/or software system placed between the Technology Resources and the Internet or to provide internal separation among Technology Resources. The primary function of a firewall is to limit unauthorized access to and use of the Technology Resources.

"Listserv" means an automatic distribution method for e-mail on the Internet. Users can subscribe to a Listserv, typically a discussion list, and receive copies of e-mail sent to the list by other subscribers.

"Policy" means this Technology Resources Policy, including all attachments.

"Server" means a computer running administrative software that controls access to a network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations connected to the network.

"Technology Resources" means BIDMC's entire computer and telecommunications network, including, but not limited to, the following: fax machines, host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, Personal Digital Assistants (PDAs), palmtop computers, software, applications, pagers, voice mail, data files, and all internal and external computer and communications networks (e.g., Internet, commercial online services, value added networks, e-mail systems) that may be accessed directly or indirectly from BIDMC's computer network or telecommunications systems. Technology Resources include assets that are located on and off BIDMC property so long as they are attached to the BIDMC serviced network or telecommunications systems.

"Users" means all employees, independent contractors, consultants, contract employees, temporary workers, and other persons or entities that use the Technology Resources, wherever they are located. This includes Users who are not affiliated with BIDMC, but who use computer and telecommunications systems maintained by BIDMC.

"Virus" means a program that infects computer files and systems, often with destructive results (e.g., loss of data, unreliable operation of infected software and systems).

"Workstation" means the individual computers assigned to one or more Users.

Policy Statement:

In using or accessing the Technology Resources, Users must comply with the following provisions:

1. **Use of Technology Resources - In General**

The Technology Resources constitute a valuable business asset of BIDMC and may only be used for approved purposes. Users are permitted access to the Technology Resources to assist them in the performance of their jobs. Occasional, limited, appropriate personal

use of the Technology Resources is permitted when the use does not: (1) interfere with the User's work performance; (2) interfere with any other User's work performance; (3) unduly impact the operation of the Technology Resources; (4) result in any material expense to BIDMC; or (5) violate any other provision of this Policy or any other policy, guideline, or standard of BIDMC.

2. Standards

The Chief Information Officer may augment this policy from time-to-time by publishing hardware, software, configuration, and practice standards. These are intended to assure Technology Resources are secure, reliable, and can be economically maintained.

3. **No Expectation of Privacy**.

Users understand and agree that:

a) BIDMC retains the right, with or without cause or notice to the User, to access or monitor the Computer Information, including User e-mail and Internet usage. Please keep in mind that anything created or stored on the Technology Resources, including the Computer Information, may be reviewed by others and that even deleted files may be recovered;

b) Users have no expectation of personal privacy of any kind related to their use of the Technology Resources or any Computer Information; and

c) Users expressly waive any right of privacy or similar right in their use of the Technology Resources or any Computer Information.

4. Ownership of Computer Information and Technology Resources

All of the Computer Information and the Technology Resources are the sole and exclusive property of BIDMC. Any User files, e-mail, or other Computer Information stored on the Technology Resources will become the property of BIDMC.

5. Prohibited Activities

5.1 Inappropriate or Unlawful Material - Content that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate, including any comments that would offend someone on the basis of race, color, religion, sex, sexual orientation, national origin, ancestry, age, disability, genetics, military service, or veteran status, or any other class protected by law, , must not be sent by e-mail or other form of electronic communication (e.g., bulletin board systems, newsgroups, chat groups), viewed on or downloaded from the Internet or other online service, or displayed on or stored in the Technology Resources. Users encountering or receiving such material must immediately report the incident to the Chief Information Officer or his/her designated representative.

5.2 Prohibited Activities - Users may not use the Technology Resources for personal financial gain or the benefit of any third party (including the sale of any non-BIDMC products or services), or to solicit others for activities unrelated to BIDMC's business, or in connection with political campaigns or lobbying. The Technology Resources may also not be used to create, store, or distribute any form of malicious

software (e.g., viruses, worms, or other destructive code).

5.3 Protection of BIDMC Data/Telecom Network - Without the express written permission of the Chief Information Officer or his/her designated representative, Users, other than authorized Information Systems employees, may not do any of the following:

a. Access the Data/Telecom Network with a diagnostic or testing tool such as a protocol analyzer intended to monitor, decode, or filter packets of information.

b. Connect a device to the Data/Telecom Network without prior coordination and approval of BIDMC Information Systems.

c. Enter a designated Data/Telecom Network equipment room without written authorization from BIDMC Information Systems.

d. Attempt to physically or logically reconfigure, move, or disengage a Data/Telecom Network component.

e. Install computer services on the Data/Telecom Network that increase BIDMC's vulnerability to denial of service attacks, viruses, or similar problems.

f. Connect remotely to the BIDMC Data/Telecom network through a modem attached to a networked PC or server.

5.4 Waste of Technology Resources - Users may not deliberately perform acts that waste Technology Resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending non-business related mass e-mailings or chain e-mail, subscribing to a non-business related Listserv, spending excessive time on the Internet, playing games, engaging in non-business related online "chat groups," or otherwise creating unnecessary network traffic.

5.5 Large File Transfers - To the extent possible, Users should schedule communications-intensive activities such as large file transfers, mass e-mailings, and streaming audio or video for off-peak times (i.e., before 7:00 a.m. and after 7:00 p.m., Monday through Friday). Because audio, video, and picture files require significant storage space, these types of files may not be transported or stored on the Technology Resources unless they are business related. All files that are downloaded must be scanned for viruses and other destructive programs.

5.6 Misuse of Licensed Software - Without prior written authorization from the Chief Information Officer or his/her designated representative; Users other than authorized Information Systems employees may not do any of the following:

a. copy BIDMC software for use on their home computers;

b. upload or transmit via e-mail any software licensed to BIDMC or data owned or licensed by BIDMC

c. provide copies of BIDMC software to any independent contractors or consultants of BIDMC or to any third person;

d. install software (including screen savers and games) or any updates to existing

software on any of BIDMC's workstations or servers;

e. download any software from the Internet or other online service to any of BIDMC's workstations or servers;

f. modify, revise, transform, recast, or adapt any software; or

g. reverse engineer, disassemble, or decompile any software.

Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to the Chief Information Officer or his/her designated representative.

5.7 Online Agreements - Without prior written authorization from the Chief Information Officer or his/her designated representative, Users may not accept or agree to be bound by any terms and conditions of use (other than standard terms and conditions of use for access to Web sites), license agreements, or other types of online agreements.

5.8 Data Transfer - Use of any software that copies BIDMC electronic patient health information to an external system is prohibited unless BIDMC has a Business Associate Agreement with the company hosting the external system.

5.9 Resource Sharing - Use of software that allows computers located in BIDMC to be shared as resources to the Internet is prohibited. For example, some P2P software allows your system to be accessed by non-BIDMC systems.

5.10 Modem Access

The use of modems to access the BIDMC's Data/Telecom Network is restricted to pre-approved situations by the Chief Information Officer. Approved modems must use a username/password combination to control access and a time-out system that terminates all idle sessions after 30 minutes. The username/password combination must adhere to the section within this policy titled "PASSWORDS".

6 **Use of Copyrighted Information.**

6.1 In General - It is the policy of BIDMC to prohibit copying or distribution of any Copyrighted Publications of third parties, except as:

a) Permitted by legal principles of "fair use" (as described in Section 6.3, below) or

b) Authorized by a contract or license that BIDMC has obtained. Copies of all contracts and licenses for Copyrighted Publications should be retained by the office administrator at the location of use and by BIDMC's legal department.

Copying may occur by using a photocopy machine, through retyping, faxing, and reprinting, as a result of storage, duplication or printing of electronic information, and through the posting of material on the Internet and other networks. Distribution may occur if Copyrighted Publications are sent through interoffice delivery, e-mail or Internet transmission (including newsgroups and other online discussion areas), client information services, etc. For example, copying an article from the New York Times Web site and

then distributing the article to a friend or client could potentially infringe several of the New York Times' exclusive rights as the owner of the copyright in the article.

6.2 Limitations of Copyright - Copyright does not necessarily protect all forms of information or printed material, particularly raw data, facts, "ideas," and "processes," and works in the public domain (e.g., works that are very old or that are specifically dedicated to the public domain), so copyright law ordinarily should not preclude Users from extracting the base factual information they need to conduct normal business activities. If a User has any questions about what is permitted, please consult BIDMC's legal department.

6.3 Fair Use - "Fair use" is a legal principle that permits a limited amount of copying of Copyrighted Publications to occur, depending on the facts and circumstances. Based on the ordinary needs of BIDMC, "fair use" will more likely occur if the following factors are present:

a) The purpose of the copying is for educational or research use;

b) The copying is a necessary step for extracting, understanding or using data or information (e.g., a necessary step in using a computer program is to copy the program into the memory of the computer);

c) The copying is to create a substantially different work, which conceptualizes, analyzes, expands upon or otherwise transforms the material being copied. This is a key element of fair use. It is one thing to simply copy an existing article and distribute it to twenty other people. It is quite another thing to take the ideas in an existing article and to expand upon them in a new article. In the first instance, there will likely be no fair use. In the later instance, the potential for fair use is high;

d) The amount of material being copied is limited to small portions, excerpts, or abstracts (e.g., if a particular paragraph in an article is of interest, do not copy the entire article);

e) The copying is not "systematic" in the sense that copies of the same or similar works are not being made repetitively, continuously, and/or in multiple quantities under circumstances that could be seen to substitute for purchases or subscriptions. The classic example of "systematic" copying is the monthly copying of the entire contents of a trade journal for circulation to every member of a particular department. That kind of activity would almost certainly not be a fair use;

f) The copying is ad hoc and as needed, conducted within BIDMC on a per-item basis, and not by commercial copy centers for large-scale distribution; and

g) Distribution of copies is strictly limited, and no fee or charge is collected for the copying or distribution.

The foregoing guidelines state some, but not all, applicable considerations, and do not preclude fair use from existing in other situations. Because every situation is judged separately, each User has final responsibility for exercising sound judgment and reasonable restraint. Each department of BIDMC, depending on need, should consider

establishing more particularized guidelines for limiting the amount of copying that occurs.

6.4 Copyright Management Information - Users may not alter Copyrighted Publications in such a way as to change, obscure, or remove information relating to the copyright owner, copyright notice information, the author of the work, the terms and conditions of use of the work, or identifying numbers or symbols referring to the foregoing information or links to such information. To the extent possible, Users should use hyperlinks to reference copyrighted material instead of making copies of such material.

6.5 Peer-to-Peer File Sharing - Users are prohibited from sharing digital audio music files, software or any other copyrighted material using BIDMC Technology Resources without the written permission of the copyright holder.

7 Use of E-mail

7.1 In General - All User e-mail addresses assigned by BIDMC shall remain the sole and exclusive property of BIDMC. Users should endeavor to make each of their electronic communications truthful and accurate. Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. The quality of your writing will reflect on BIDMC. Always strive to use good grammar and correct punctuation. Never send a message in the "heat of the moment." Always allow time to reflect before composing a message. The following etiquette guidelines should be followed in drafting e-mail:

a) Avoid using all capitals;

b) Avoid excessive use of bold faced type;

c) Only mark high priority items as "Priority";

d) Avoid copying unnecessary parties with the "Reply All" feature;

e) Make the subject line for your e-mail descriptive;

f) Avoid using graphic backgrounds for your e-mail and ornate type fonts. These will make your e-mail less readable and will require far greater company resources to store and transmit than ordinary e-mail; and

g) Do not send messages to all users or other large groups within the company unless absolutely necessary.

7.2 Altering Attribution Information - Users may not alter the "From" line or other attribution of origin information in e-mail or other online postings. Anonymous or pseudonymous electronic communications are forbidden.

7.3 Forwarding E-mail - Users should use their good judgment in forwarding e-mail to any other person or entity. When in doubt, request the sender's permission to forward the message. E-mail containing Confidential/Proprietary Information or attorney-client communications may never be forwarded without the permission of the sender or other authorized personnel. All messages written by others should be forwarded "as-is" and with no changes, except to the extent that you clearly

indicate where you have edited the original message (e.g., by using brackets [ ] or other characters to indicate changes to the text).

7.4 Confidential/Proprietary Information - Each User must take all appropriate precautions to insure that Confidential/Proprietary Information is not improperly disclosed or otherwise compromised by transmission via e-mail. If this information is transmitted via e-mail, the sender of the message is responsible for: (i) insuring that the e-mail is clearly labeled in the subject line and the body of the message as "Confidential", "Proprietary," "Confidential: Unauthorized Use or Disclosure is Strictly Prohibited" or "Privileged Attorney-Client Communication"; (ii) keeping the address list for the e-mail to a minimum; (iii) insuring all recipients are aware of the obligation to maintain the confidentiality of the information contained in the e-mail; and (iv) assuring that the transmission of information is in accordance with this Policy and applicable law.

7.5 Unauthorized Receipt of Confidential/Proprietary Information - In the event a User receives e-mail, whether designated as confidential or not, by mistake, the User should stop reading the message and immediately notify the sender or system administrator. It is a violation of this Policy to read e-mail intended for another person without the express prior consent of that person or other authorized BIDMC personnel.

7.6 Listserv Subscriptions - Users should be selective in subscribing to listservers and other e-mail distribution lists. Some discussion groups are very active and may result in dozens of e-mail every day. Promptly unsubscribe to any listservers that you are not actively reading. When subscribing to a listserv, make sure to keep a record of the steps necessary to cancel the subscription. This information is usually contained in an initial message from the listserv, but may not be easily located later.

7.7 Access to E-mail Through Third Party Services - Users are cautioned that external email systems usually lack sufficient security to maintain the privacy of an electronic discussion. Therefore, Users should not store or send sensitive patient or business information over systems not maintained by BIDMC unless appropriate encryption is in place.

7.8 Retention and Destruction of E-mail - Users should exercise good housekeeping practices with regard to their central e-mail account. Email that is no longer needed should be purged. This minimizes storage cost. It also improves backup and file recovery cycle time. If an email needs to be retained as a permanent or lasting record, the User shall print the e-mail and retain it in accordance with BIDMC's Records Management Policy. Deleted email will, generally, not be recovered. Users are expected to use caution when deleting email as it may not be recoverable if permanent deletion has occurred.

7.9 E-mail Forwarding - Automatic forwarding of email to a third party system is not permitted. It places an administrative burden on Information Systems and can result in sensitive information being compromised in transit via the Internet. In exceptional cases, as approved by a VP and the CIO, email forwarding may be done for temporary periods. Exceptions will typically be limited to situations where the communication lines to the receiving facility are secured through physical or virtual private connections.

8 **Internet Access and Use**

8.1 Authorized Uses - Users are encouraged to use the Internet and intranets to assist them in the performance of their jobs. Authorized uses include, but are not limited to, the following:

a) Patient services, human resources, education, and research;

b) Electronic communication; and

c) Professional purposes and procurement of information from external sources.

8.2 Internet Monitoring - BIDMC has software and systems in place that are capable of monitoring and recording Internet usage. These security measures may be capable of recording Web sites visited, chat, newsgroup, or e-mail message, and each file transfer into and out of BIDMC's networks. BIDMC reserves the right to conduct such monitoring and recording at any time. As described in Section 2, Users have no expectation of privacy as to their Internet usage. BIDMC may review Internet activity and analyze usage patterns, and may choose to publicize this data to assure that the Technology Resources are used in accordance with the provisions of this Policy.

8.3 Chat Groups and Newsgroups - Internet Chat Groups and Newsgroups are public forums where it is inappropriate to discuss or reveal confidential information, patient data, trade secrets, and any other Confidential/Proprietary Information. Users must identify themselves honestly, accurately, and completely when participating in chat groups, newsgroups, and when setting up accounts on outside computer systems. Only those Users who have been duly authorized by BIDMC may speak/write in the name of the company when making postings to chat groups or newsgroups. Other Users may participate in chat groups and newsgroups, provided (i) participation will assist them in the performance of their jobs, and (ii) the following footer is included on all postings or comments: "This posting reflects the individual views and opinions of the author and does not necessarily represent the views and opinions of BIDMC." Users should understand that each of their postings will leave an "audit trail" indicating at least the identity of BIDMC's Internet servers, and, most likely, a direct trail to the User. Inappropriate postings may damage BIDMC's reputation and could result in corporate or individual liabilities. Accordingly, Users must use every effort to be professional in making comments online.

8.4 Accessing the Internet - To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to BIDMC's Data/Telecom Network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, from a workstation is strictly prohibited unless the computer is not connected to the network (e.g., a laptop being used remotely). Even if a stand-alone computer with a modem is used to access the Internet or other network, the modem must never be left in auto-answer mode.

8.5 Disclaimer of Liability for Internet Use - BIDMC IS NOT RESPONSIBLE FOR MATERIAL VIEWED OR DOWNLOADED BY USERS FROM THE INTERNET. THE INTERNET IS A WORLDWIDE NETWORK OF COMPUTERS THAT CONTAINS MILLIONS OF PAGES OF INFORMATION. USERS ARE CAUTIONED THAT MANY OF THESE PAGES INCLUDE OFFENSIVE, SEXUALLY EXPLICIT, AND INAPPROPRIATE MATERIAL. IN GENERAL, IT IS

DIFFICULT TO AVOID AT LEAST SOME CONTACT WITH THIS MATERIAL WHILE USING THE INTERNET. EVEN INNOCUOUS SEARCH REQUESTS MAY LEAD TO SITES WITH HIGHLY OFFENSIVE CONTENT. IN ADDITION, HAVING AN E-MAIL ADDRESS ON THE INTERNET MAY LEAD TO THE RECEIPT OF UNSOLICITED E-MAIL CONTAINING OFFENSIVE CONTENT. USERS ACCESSING THE INTERNET DO SO AT THEIR OWN RISK.

9 **Passwords**.

9.1 Responsibility for Passwords - Users are responsible for safeguarding their passwords for access to the Technology Resources. Users should recognize that the combination of a logon identification and password is the equivalent of a signature and that the disclosure to another individual is the equivalent of handing that individual a signed blank check. Individual passwords should not be printed, stored on-line, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system using another User's password or account.

9.2 Password Guidelines – To the extent the software application supports them, users should follow these guidelines when choosing a password:

a) Each password will be not less than 8 characters in length.

b) Passwords must comply with at least three of these four rules:

(1) English upper case letters – A, B, C, …Z
(2) English lower case letters – a, b, c, …z
(3) Westernized Arabic numerals – 0, 1, 2, …9
(4) Non-alphanumeric "special characters" - #, &, etc.

c) The password is to be changed frequently or whenever a compromise of the password is suspected.

d) A password may not be reused in less than 6 months.

e) Passwords should not be associated with personal information (e.g., PIN used for bank cards, date of birth for self or family members, telephone numbers, first or last name of self or family members, passwords used for Internet accounts).

9.3 Passwords Do Not Imply Privacy - Use of passwords to gain access to the Technology Resources or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the Technology Resources. BIDMC has global passwords that permit it access to material stored on its computer system -- regardless of whether that material may have been encoded with a particular User's password.

10 **Security**.

10.1 Accessing Another User's Files - Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of that file. The ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of others by unnecessarily reviewing their files and

e-mail.

10.2 Accessing Other Computers and Networks - A User's ability to connect to other computer systems using the Technology Resources or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

10.3 Control of Media - Users having magnetic media for tape units attached to their hardware or utilizing floppy disks, zip disks, CD's, USB drives and other removable media (collectively, "Removable Media") will establish procedures to label, account for, and control all media containing BIDMC data or information, regardless of whether such data or information is current or obsolete. Removable Media in the possession of Users will be stored in locked cabinets or locked desk drawers and should never be left unattended. Removable Media must be disposed of in accordance with procedures provided by BIDMC policy. If removable media contains EPHI or BIDMC sensitive information, the data must be secured at a minimum with a password.

10.4 Remote Access - BIDMC provides several methods of remote access. For business-to-business connections such as those used by outside vendors to provide remote maintenance support, a Virtual Private Network (VPN) connection will be used. For employees and staff who wish to access systems from home or other off-site locations, web services using SSL encryption or Metaframe are the preferred connection methods. Access to these services can be requested through the IS Support Call Center. When accessing hosts inside the BIDMC firewall from external locations, no exception to these connection methods will be allowed unless approved by the Chief Information Officer or his/her designee.

10.5 Use of Remote Access Software - The installation, set-up and use of software that provides a remote User control of an in-house desktop computer requires the prior approval of the Chief Information Officer or his/her designated representative. Such installation, set-up and use, if approved, will be required to adhere to any additional procedures specified by Information Systems to restrict and control access.

10.6 Network Admission - Before a device connects to the BIDMC data network, it must comply with safe network admission practices. These ensure a device will not introduce security vulnerabilities, spread malicious software, or do other harmful actions that jeopardize business operations or sensitive information. Safe practices include having up-to-date software patches, activated and up-to-date antivirus software, and no unnecessary services running on the device. If the device is not under central IT management, it must also have an able administrator assigned. Devices connected must be maintained as new security vulnerabilities arise and best practices change. Non-compliant systems will have their network port disabled.

10.7 Outside Access Computer Security - Each User is responsible for ensuring that his or her use of outside computers and networks, like the Internet, will not compromise the security of the Technology Resources. This duty includes taking reasonable precautions to prevent intruders from accessing BIDMC's network without authorization and to prevent the introduction and spread of viruses. When accessing BIDMC computer resources from home or other off-site location, users

are expected to exercise reasonable precautions to ensure they are doing so in a safe manner. This includes keeping their local computer free of spyware, keystroke grabbers, and similar threats.

10.8 Wireless Devices - Before installing any radio frequency (RF) transmitters on BIDMC owned or leased property, Users will coordinate with Clinical Engineering. This is necessary to assure the device will not interfere with other installed devices including sensitive electronic medical equipment. Information Systems approval must also be obtained before introducing RF sources that impact telecommunications or data network services such as Bluetooth or WiFi devices.

10.9 Mobile Device Use - Users granted access to BIDMC mobile computers for remote access to BIDMC applications are responsible for insuring that unauthorized persons are prevented from using the device, accessing files stored on the device, or using the device to gain access to BIDMC's network. In particular, a mobile device should never be left unattended in any uncontrolled environment (e.g., in a hotel room, at a vendor's facility, or at any other remote location). If need be and conditions permit, the device should be locked in a hotel safe or the trunk of a car or kept in the User's possession. Power-up and time-limited screensaver password protection must be enabled on mobile devices. If the User's device is lost or stolen or if a User believes that a password has been compromised, report the incident immediately to the Chief Information Officer or his/her designated representative.

10.10 HIPAA Security Regulations – Any device containing electronic patient health information, as defined by HIPAA and supplemented by BIDMC privacy policies shall comply with HIPAA security regulations. Additionally, User will comply with other BIDMC privacy policies including, but not limited to PV-03 "Managing Access to Computer Systems within the BIDMC OHCA", PV-07 "Safeguarding Protected Health Information" and PV-22 "HIPAA Security Policy".

11 **Viruses**

11.1 Virus Detection Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the Technology Resources and for timely reporting discovered viruses to the IS Support Center (617-754-8080). To that end, all material received on floppy disk or other magnetic or optical media and all material downloaded from the Internet or from computers or networks that do not belong to BIDMC MUST be scanned for viruses and other destructive programs before being placed onto the Technology Resources. Users should understand that their home computers and/or laptops might contain viruses. All disks transferred from these computers to the Technology Resources MUST be scanned for viruses.

11.2 Approved Virus Software Only Information Systems approved virus scan software is to be used for scanning for viruses. Users may obtain copies of the approved virus scan software from the IS Support Center (617-754-8080) for use on BIDMC computers and laptops.

11.3 Preventing the Spread of Viruses To prevent the spread of viruses, every User must do the following:

a) Obtain prior approval of the IS Support Center before installing or loading any

software or data, including demos, shareware, or freeware, on any of BIDMC's workstations or servers;

b) Obtain prior approval of the IS Support Center before downloading, transmitting, or otherwise electronically exchanging computer files with sources outside of the BIDMC system;

c) In the event a User discovers a virus, the User must not forward the file on to any other user. Instead, the User must immediately report the virus to the IS Support Center; and

d) Avoid using disks and other removable storage media on more than one computer system.

e) When accessing BIDMC computer resources from off-site via a VPN or other trusted connection, ensure the device from which you are connecting has up-to-date software security patches and anti-virus software installed.

12 **Encryption Software.**

12.1 Use of Encryption Software Users may not install or use encryption software on any of BIDMC's computers without first obtaining written permission from the Chief Information Officer or his/her designee. Users may not use passwords or encryption keys for encryption purposes that are unknown to their supervisors.

12.2 Export Restrictions The federal government has imposed restrictions on the export of programs or files containing encryption technology (e.g., e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology may not be placed on the Internet or transmitted in any way outside the United States without prior written authorization from the Chief Information Officer or his/her designee.

13 **Disclosures Regarding Security Issues**

Information relating to virus attacks, hacking incidents, and other breaches of security shall be treated as highly confidential. Unless specifically directed to do so by the Chief Information Officer or his/her designee, Users may not discuss this information with their co-workers or disclose it to any non-employee. The User will consider violations of this provision a serious breach of trust.

14 **Miscellaneous.**

14.1 Compliance with Applicable Laws and Licenses. In their use of the Technology Resources, Users must comply with all software licenses, copyrights, and all other state, federal, and international laws.

14.2 Other Policies Applicable. In their use of the Technology Resources, Users must observe and comply with all other policies and guidelines of BIDMC.

14.3 Amendments and Revisions. This Policy may be amended or revised by BIDMC from time-to-time as deemed necessary. Users will be provided with copies of all amendments and revisions.

14.4 No Additional Rights. This Policy is not intended to, and does not grant, Users any contractual rights.

Vice President Sponsor: John Halamka, Chief Medical Information Officer

Approved By:
☒ Operations Council: 10/1/2007 **Eric Buehrens**
Chief Operating Officer

Requestor Name: John Halamka, Chief Medical Information Officer

Original Date Approved: 10/01

Next Review Date: 10/1/2010

Revised: 09/10/2007

Eliminated:

References: